

Technology Review

DAS MAGAZIN FÜR INNOVATION

Computer

Endlich wird
IT-Sicherheit
nutzerfreundlich

Gen-Pflanzen

Monsanto will
Erbgut-Moleküle
spritzen

Künstliche
Intelligenz
Wie klug
wird
Facebook?

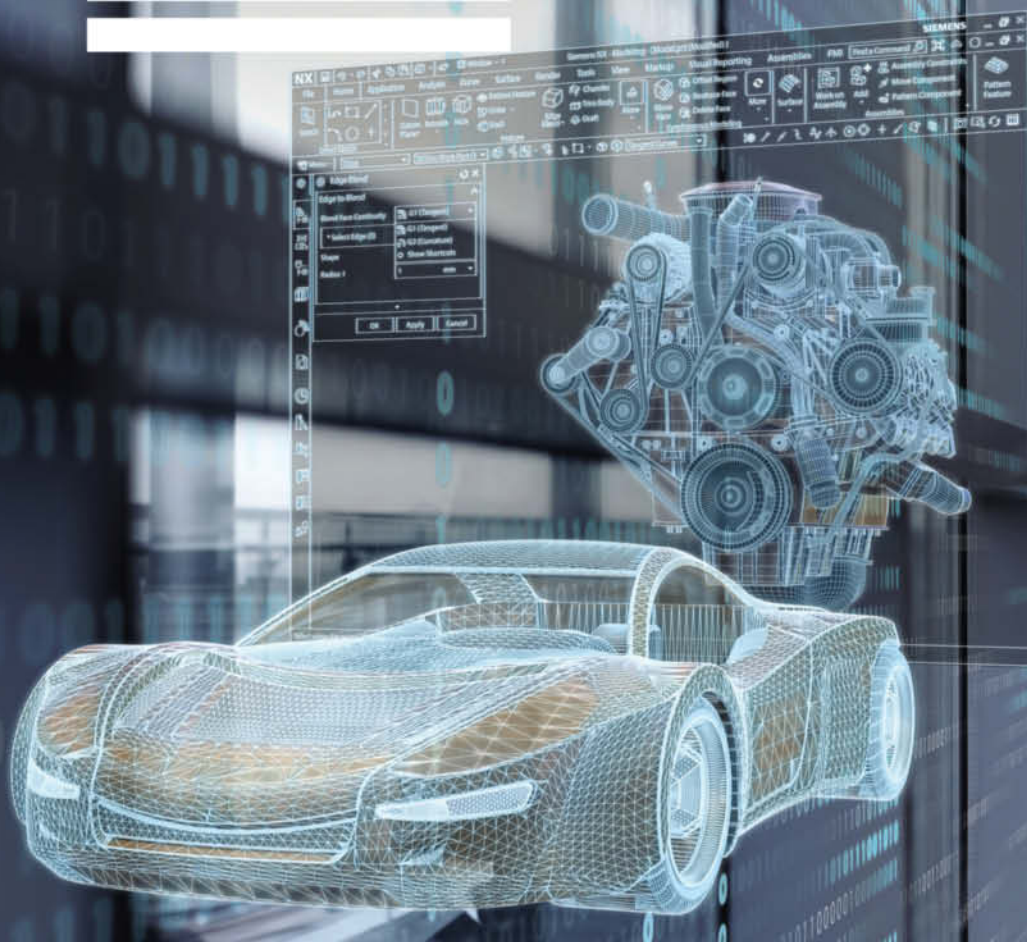


Der nächste Goldrausch?

Warum Banken plötzlich Bitcoins lieben: Über Krypto-Genies, Finanzjongleure – und die Zukunft des Geldes



SIEMENS



Realisieren Sie Leidenschaft.

Siemens PLM Software: Branchenlösungen für "Smart Innovation".

In unserer Welt smarter, vernetzter Produkte können ganze Märkte durch eine einzige Innovation verschwinden. Wie wollen Sie da erfolgreicher werden? Herkömmliche Maßstäbe für Erfolg – Qualität, Kosten, Geschwindigkeit – gelten nicht mehr. Die besten Lösungen von heute werden morgen veraltet sein. Vorausdenkende Unternehmen digitalisieren ihren gesamten Innovationsprozess, von der Entwicklung über die Herstellung bis zur Anwendung. Es reicht nicht, eine gute Idee zu haben, man muss sie auch verwirklichen können.

Dabei helfen wir. Unser Smart Innovation Portfolio bringt Sie auf den Weg zum "Digitalen Unternehmen." Damit sind Sie bestens aufgestellt, um bahnbrechende Innovationen auf den Markt zu bringen – oder darauf zu reagieren.



Das Smart Innovation Portfolio ist ein anpassbares System. Dadurch erhält jeder Beteiligte die richtigen Informationen zur richtigen Zeit im richtigen Format – in intelligenten digitalen Produktmodellen, die entlang der kompletten Wertschöpfungskette mit Informationen angereichert werden, um selbstständig ihre Herstellung und Anwendung zu optimieren.



LIEBE LESERINNEN UND LESER,

VIELE REDEN

von der Digitalisierung und denken doch nur an das nächste Geschäftsmodell. Dabei steckt weit mehr dahinter: Die Digitalisierung ist die Rebellion der Moderne. Der Antrieb hinter neuen Ideen von 3D-Druck bis Streaming war nie nur rein kapitalistisch. Es war ebenso die unbändige Freude daran, die etablierte Wirtschaft herauszufordern, ihrer Selbstgewissheit den Boden unter den Füßen wegzuziehen. Dahinter steckt **der Geist der Hacker**, die Cypherpunk-Bewegung. Ihr Traum einer egalitären, antiautoritären, bisweilen radikallibertären Gesellschaft ist natürlich Utopie pur, und ob man sie in allen Punkten teilen will, sei dahingestellt. Aber dort entstand die Haltung, alles infrage zu stellen, der bisweilen schon pubertäre Wille zur Disruption. Es wird nicht mehr protestiert, sondern programmiert – und die Alternative ins Netz gestellt. Wer den Geist der Cypherpunk-Bewegung nicht versteht, begreift auch den heutigen Fortschritt nicht, im Guten wie im Schlechten.

Ein gutes Beispiel ist die Geschichte des Bitcoins: Hätte ihr mysteriöser Begründer Satoshi Nakamoto nicht von einem **Gegenmodell zum globalen Finanzsystem** geträumt, die Kryptowährung würde wohl bis heute nicht existieren. Inzwischen arbeiten Banken daran, mit der Technologie das Geldsystem zu verändern (Seite 26). Der Aufstieg des Bitcoins war der Weckruf. Plötzlich merkte eine ganze Branche, dass ihr Geschäft angreifbar ist und dringend einer Erneuerung bedarf.

Die Zukunft wird zeigen, ob die Finanzwelt damit transparenter und kontrollierbarer wird – oder ob das alte Spiel einfach nur mit neuer Technologie weitergeht. Dieses Risiko steckt jedoch hinter jeder Innovation. Nur weil sich etwas ändert, wird es noch lange nicht gut. Ob etwa der US-Agrochemiekonzern Monsanto mit seinem **neuen Gen-Spray** wirklich der Umwelt und den Landwirten hilft, ist heftig umstritten (Seite 46). Aber wenn sich nichts ändert, wird es auch nicht besser.

Ich begrüße Sie in unserer Oktober-Ausgabe.

Ihr

Robert Thielicke

10.2015 INHALT

Rot gefärbte
Themen sind auf
der Titelseite
angekündigt.

Technology Review ist die
deutsche Ausgabe des gleichnamigen
Magazins vom Massachusetts
Institute of Technology MIT.

36 WOHNEN AUF KUFEN

Eine futuristische Antarktis-
Station setzt neue archi-
tektonische Maßstäbe.



42 WIE KLUG WIRD FACEBOOK?

Mit künstlicher Intelligenz und Maschinenlernen will Yann LeCun das
soziale Netzwerk zum digitalen Assistenten für den Alltag machen.



66 IT-SICHERHEIT

Das Zeitalter der Massenhacks hat begonnen.
Gibt es überhaupt noch Schutzmaßnahmen?

46 GENTECH ÜBER BANDE



Der US-Konzern
Monsanto will
Schädlingen wie dem
Kartoffelkäfer
beikommen, indem er
RNA-Schnipsel versprüht.
Wie sicher ist das?



52 NEUSTART AUF VIER RÄDERN

Apple und Google liefern sich mit Fahrzeugherstellern ein Wettrennen um das künftige Betriebssystem für Autos.

Fotos: Antony Dubber, Thomas Ehretsmann, Fotolia, Stephen Russell/Stanford University Dynamic Design Lab, Illustration: Alex Williamson; Cover: shutterstock.de



EINBLICK

8 **ENERGIE** Kernfusion „Made in Germany“



AKTUELL

10 **MEDIZIN** Neuer Ansatz für mehr Organspenden
12 **VERKEHR** Ampeln verraten, wie lange sie noch rot sind
15 **MEDIZIN** Künstliche Virenpartikel bekämpfen Bakterien
16 **ESSEN** Fruchtgummi aus dem 3D-Drucker
19 **MATERIAL** Proteine bringen Dioden zum Leuchten
20 **LUFTFAHRT** Laserkanone holt Drohnen vom Himmel



AM MARKT

22 **E-AUTOS** Der dritte Tesla kommt
23 **OUTDOOR** Schlafsack, Liegematte und Zelt in einem
24 **REIFEN** Absolut wartungsfrei und pannensicher
25 **AUSPROBIERT** Fahrrad für Hand und Fuß



HORIZONTE

26 **BITCOIN** Banken entdecken den Charme der Anarcho-Währung
34 **MEDIZIN** Ärzte haben eine neue Waffe: kaltes Plasma
36 **ARCHITEKTUR** Forschungsstation auf Skiern
42 **NEURO-NETZE** So will Facebook schlauer werden
46 **GENTECH** RNA-Sprays entfachen die nächste große Debatte
52 **VERKEHR** Apple und Google haben das Auto im Visier



TR MONDO

58 **USA** Drohnen überwachen Stadionbaustelle
63 **JAPAN** Der stärkste Laser der Welt leistet zwei Milliarden Watt
64 **PHILIPPINEN** Meerwasser lässt Lampe leuchten



FOKUS
IT-SICHERHEIT

66 **TREND** Das Zeitalter der Massenhacks hat begonnen
70 **INTERVIEW** So lassen sich die Täter fassen
72 **SPIONAGE** Die USA erheben erstmals offiziell Anklage
78 **USABILITY** Sicherheit geht auch bequem
82 **RECHT** Auch „gute“ Hacker leben in gesetzlicher Grauzone



MEINUNG

84 **MYTHEN** Warum der Glaube an große Technikhelden schadet
88 **BÜCHER** Marc Goodman über die Verbrechen der Zukunft



ZU „KAMERA MIT BLICK FÜRS BÖSE“
(6/2015)

Die Gedanken sind nicht mehr frei

Der erste Schritt zum Gedankenverbrechen ist das angebliche Erkennen krimineller Gedanken. Falls sich so ein System bewähren sollte, ist es nur eine Frage der Zeit, bis Politiker eine Art 3-Strikes-Strafrecht fordern, um jene hinter Gitter zu bringen, bei denen es dreimal angeschlagen hat. Natürlich ist ein Missbrauch programmiert. Kein System ist jemals perfekt.

ALEX KLOSS

ZU „BIOGAS AUS DER HAUSANLAGE“
(8/2015)

Warum kein Gasspeicher?

Mal ist zu viel Gas da, und die Bewohner müssen kochen, damit es nicht ungenutzt entweicht. Dann ist wieder zu wenig da. Warum wird das Gas nicht gespeichert? Man bräuchte lediglich einen Kompressor und ein paar Gasflaschen. Der Vorteil wäre, dass man in den Flaschen das Gas auch an andere Haushalte verkaufen kann. Klar braucht der Kompressor etwas Strom. Sollte dort kein Netzstrom verfügbar sein, könnte man ihn per kleinem Generator, der das Biogas nutzt, oder per Photovoltaik erzeugen.

HENKO VIA TR ONLINE



ZU „UNBEGRENZT ELEKTRISCH“ (9/2015)

Mehr Technik, weniger Design

Ich bin seit vielen Jahren Leserin Ihrer Zeitschrift – der Technik wegen. Dann kam dieser Artikel. Mich hätten technische Details über die Umsetzung des Antriebs interessiert, nicht das Design. Stattdessen referiert Herr Schwarzer nach einer kurzen Einführung darüber, dass der neue Toyota Mirai nicht seinen Geschmack trifft. Das wäre auch mit einem Satz dem Leser zur Kenntnis gelangt. Herr Schwarzer braucht dafür jedoch vier. Es folgt eine vage Passage über das Bedienen des Fahrzeugs, die ich eventuell in der „Auto Bild“ vermutet hätte. Im zweiten Drittel hatte ich dann doch noch die Hoffnung, irgendein nicht bekanntes, neues Detail zu erhaschen, zum Beispiel über den Tank, der weniger Fluktuation beim Wasserstoff hat. Dumm gelaufen, aber die Hoffnung stirbt ja bekanntermaßen zuletzt. Genau da verweist der Protagonist auf den BMW i8 – ein Fahrzeug, das mit einem Ottomotor arbeitet – aber dessen Design „schöner“ ist. Liebe Redaktion: Leser kaufen eure Zeitschrift wegen der breiten technologischen Übersicht und wollen Technik sehen und davon lesen.

JENNIFER SIRTIL



ZU „DAS ERBE DES UFOS“ (9/2015)

Korrektur

In dem Artikel sind uns leider zwei Fehler unterlaufen. Zum einen schrieben wir irrtümlich, dass die Entwicklungskosten des Lockheed-Martin-Kampffjets 60 Millionen Dollar betrugen. Korrekt sind 60 Milliarden. Zum anderen heißt das auf dem Markt befindliche Kampffjet-Modell korrekt F-35B, nicht X-35B. Als X-35B wurde nur der Prototyp bezeichnet. Wir bitten die Fehler zu entschuldigen.
Die Redaktion



SCHREIBEN SIE AN:

LESERBRIEFE@TECHNOLOGY-REVIEW.DE

Die Redaktion behält sich vor,
Einsendungen zu kürzen



iX Cloud-Konferenz 2015



Foto: © ristaumedia.de – Fotolia.com

Cloud-Dienste bauen, nutzen & optimieren

Eigenes RZ, Hybrid-Cloud oder paketierte Dienste

Unternehmensdaten im eigenen Rechenzentrum vorzuhalten oder in die Cloud auszulagern ist nicht nur eine Frage der Sicherheitsanforderungen, sondern auch der Abwägung der Kosten-Nutzen-Relation.

Frühbuchergebühr: 484,50 Euro (inkl. MwSt.)

Standardgebühr: 570,00 Euro (inkl. MwSt.)

VERANSTALTUNGSORT: Kassel

Themenvorschau:

- Hybrid-Cloud – Brückenschlag zwischen den IT-Welten
- Cloud im Eigenbau: Sicher betreiben und skalieren
- Verschlüsselung für Cloud-Dienste – Anbieter und Konzepte im Vergleich
- Software-defined Storage/Network – das Management im Griff
- Kosten-Nutzen-Vergleich: Lokales RZ versus Cloud-Dienste
- Praxis: Private Cloud, Hybrid Cloud oder Public Cloud
- Recht: Stolperfallen im Admin-Alltag vermeiden

**SAVE
THE DATE**
25. November
2015

Eine Veranstaltung von:



Organisiert von:



Weitere Informationen und Anmeldung unter: **www.heise-events.de/clouddienste2015**

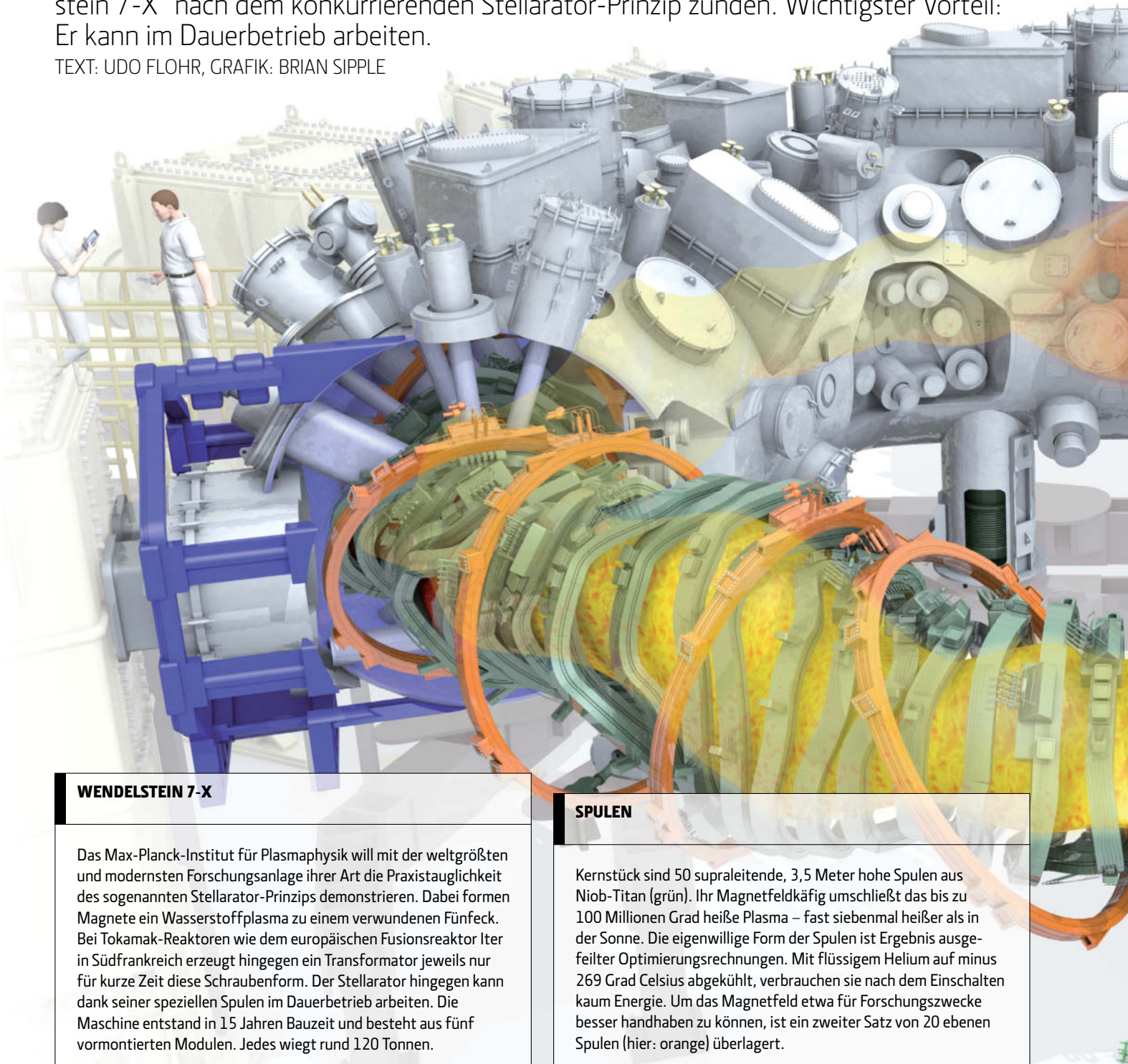
Nutzen Sie die Möglichkeit zur PGP-Zertifizierung: **www.ct.de/pgp**



Sonne im Käfig

Greifswald ist das kleine gallische Dorf der Plasmaphysik: Während alle Welt versucht, Fusionsreaktoren des Tokamak-Typs zu bauen, soll dort noch dieses Jahr der „Wendelstein 7-X“ nach dem konkurrierenden Stellarator-Prinzip zünden. Wichtigster Vorteil: Er kann im Dauerbetrieb arbeiten.

TEXT: UDO FLOHR, GRAFIK: BRIAN SIPPLE



WENDELSTEIN 7-X

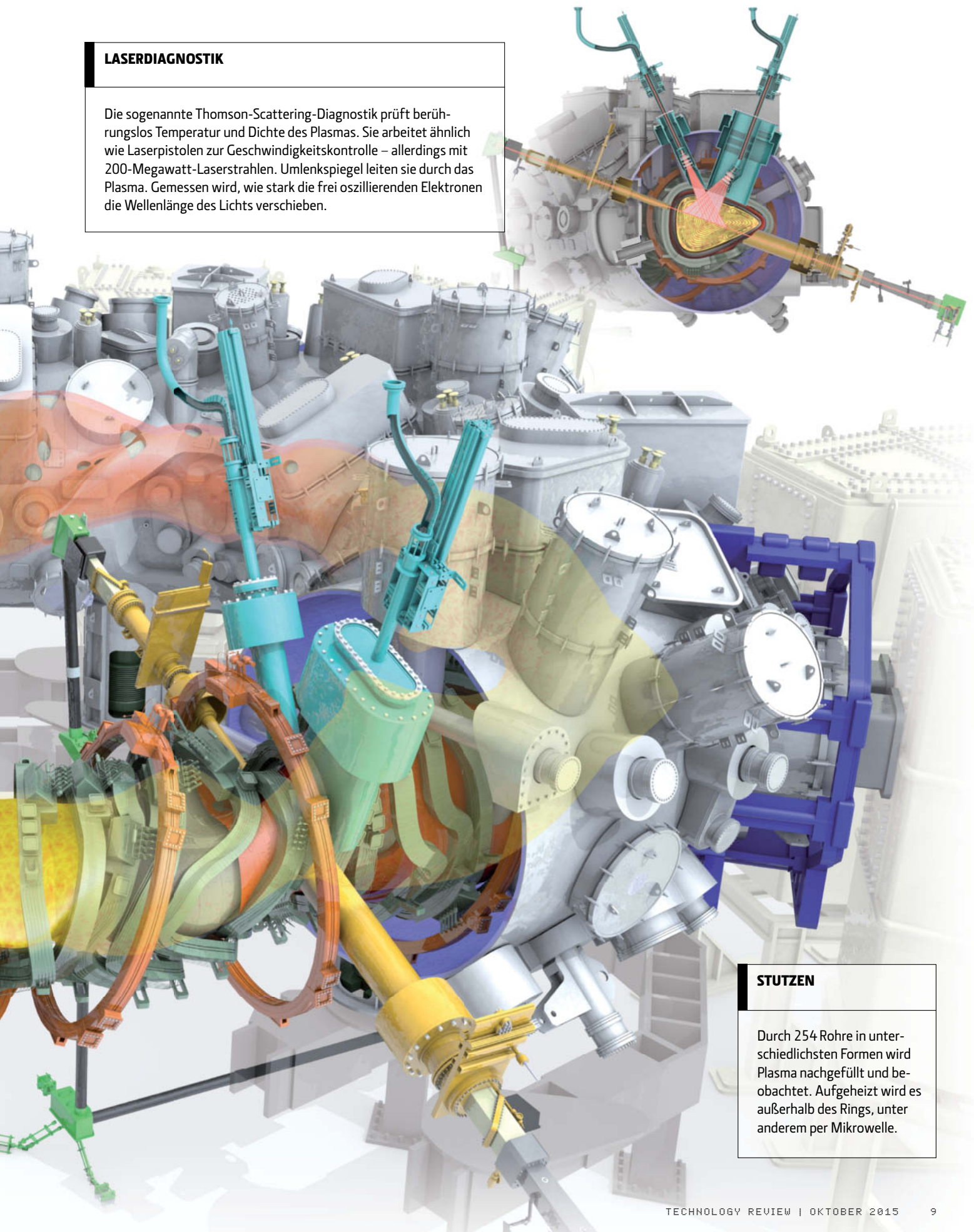
Das Max-Planck-Institut für Plasmaphysik will mit der weltgrößten und modernsten Forschungsanlage ihrer Art die Praxistauglichkeit des sogenannten Stellarator-Prinzips demonstrieren. Dabei formen Magnete ein Wasserstoffplasma zu einem verwundenen Fünfeck. Bei Tokamak-Reaktoren wie dem europäischen Fusionsreaktor Iter in Südfrankreich erzeugt hingegen ein Transformator jeweils nur für kurze Zeit diese Schraubenform. Der Stellarator hingegen kann dank seiner speziellen Spulen im Dauerbetrieb arbeiten. Die Maschine entstand in 15 Jahren Bauzeit und besteht aus fünf vormontierten Modulen. Jedes wiegt rund 120 Tonnen.

SPULEN

Kernstück sind 50 supraleitende, 3,5 Meter hohe Spulen aus Niob-Titan (grün). Ihr Magnetfeldkäfig umschließt das bis zu 100 Millionen Grad heiße Plasma – fast siebenmal heißer als in der Sonne. Die eigenwillige Form der Spulen ist Ergebnis ausgefeilter Optimierungsrechnungen. Mit flüssigem Helium auf minus 269 Grad Celsius abgekühlt, verbrauchen sie nach dem Einschalten kaum Energie. Um das Magnetfeld etwa für Forschungszwecke besser handhaben zu können, ist ein zweiter Satz von 20 ebenen Spulen (hier: orange) überlagert.

LASERDIAGNOSTIK

Die sogenannte Thomson-Scattering-Diagnostik prüft berührungslos Temperatur und Dichte des Plasmas. Sie arbeitet ähnlich wie Laserpistolen zur Geschwindigkeitskontrolle – allerdings mit 200-Megawatt-Laserstrahlen. Umlenkspiegel leiten sie durch das Plasma. Gemessen wird, wie stark die frei oszillierenden Elektronen die Wellenlänge des Lichts verschieben.



STUTZEN

Durch 254 Rohre in unterschiedlichsten Formen wird Plasma nachgefüllt und beobachtet. Aufgeheizt wird es außerhalb des Rings, unter anderem per Mikrowelle.



aktuell

Das „Organ Care System“ versorgt ein Herz mit Sauerstoff und Nährstoffen.

Neues Leben für tote Herzen

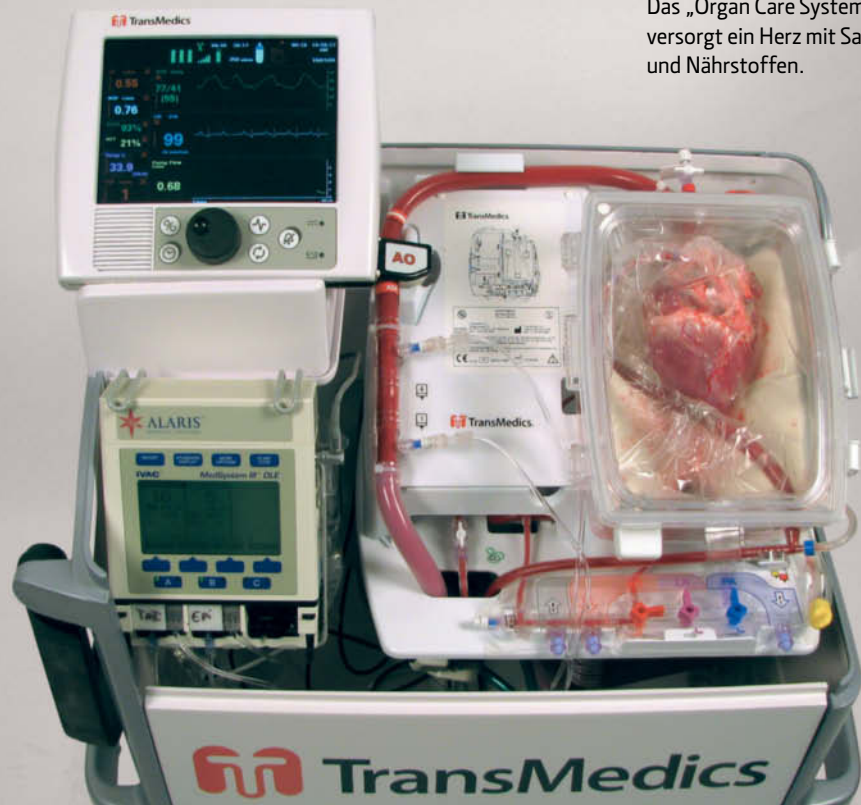


Foto: TransMedics

Weil es zu wenige Spenderherzen gibt, pöppeln Ärzte auch die Pumporgane bisher ungeeigneter Spender mit einer Maschine wieder auf.

Im März bekam Huseyin Ulucan nach sieben Jahren Warten endlich ein neues Herz. Sein eigenes war durch einen Herzinfarkt stark geschädigt. „Vor der Operation konnte ich kaum laufen und kam schnell außer Puste. Ich hatte keine gute Lebensqualität mehr“, sagt er. Er hätte womöglich noch viel länger warten müssen, hätten sich Mediziner am Papworth Hospital in Großbritannien nicht zu einem ungewöhnlichen Schritt entschlossen: Sie transplantierten ihm als erstem europäischen Patienten das Herz eines kurz zuvor an Herzstillstand gestorbenen Spenders, das ein Spezialgerät frisch hielt. In Deutschland sind solche Spenden von sogenannten „non-beating heart donors“ nicht erlaubt. Erst nach dem Hirntot ist eine Organentnahme legal.

Pumporgane von Patienten, die an Herz- oder Kreislaufversagen gestorben sind, galten bisher unter Chirurgen als zu beschädigt für eine Transplantation. Denn wenn ein Herz zu schlagen aufhört, fehlt es ihm an Sauerstoff, und seine Muskelzellen beginnen abzusterben. Ohne Gegenmaßnahmen und bei Raumtemperatur schreitet dieser Verfall schnell voran. Normalerweise werden daher nur die Herzen von hirntoten Spendern verpflanzt, deren Körper bei der Entnahme noch am Leben ist. Doch es gibt nicht genug Spender, sagt der Chirurg Stephen Large vom Papworth Hospital. Huseyin Ulucan hatte Glück: „Ich fühle mich täglich stärker. Heute Morgen bin ich ohne Probleme ins Krankenhaus gelaufen“, erzählte er kurz nach dem Eingriff der britischen Zeitung „The Telegraph“.

Larges Team benutzte ein sogenanntes „Organ Care System“ (OCS) des US-Unternehmens Transmedics, um das für Ulucan gedachte Spenderherz bis zur Transplantation zu

versorgen. In der mobilen Maschine lassen sich Herzen und Lungen außerhalb des Körpers funktionsfähig halten – und zwar mit zwölf Stunden dreimal länger als mit der üblichen Kühlung bei vier Grad (s. TR 1/2012, S.10). Die OCS, die in Europa und Australien kommerziell erhältlich sind und in den USA auf die Zulassung warten, haben noch einen zweiten Vorteil: Sie können auch geschwächte Organe wieder aufpäppeln, die sonst nicht kräftig genug für eine Transplantation wären. In der 250.000 Dollar teuren Maschine wird das Spenderherz in einer sterilen Kammer über Schläuche mit körperwarmem Blut, also mit Nährstoffen und Sauerstoff versorgt.

Durch „non-beating“-Spender könnte die Zahl der verwendbaren Herzen laut Large um bis zu 30 Prozent steigen. Es ließen sich also mehr Menschen retten, die sonst an Herzversagen sterben würden. In Großbritannien wurde das System seit Huseyin Ulucan in zehn weiteren Fällen eingesetzt. Sechs weitere Operationen fanden in Australien statt.

Neben Transmedics arbeiten auch andere Unternehmen an Organ-Versorgungsmaschinen: etwa Organ Assist in den Niederlanden, OrganOx in Großbritannien sowie Organ Solutions in den USA. Organ Solutions' Maschine soll Lebern von verstorbenen Spendern versorgen. Geschäftsführer Korkut Uygun hofft, dass mit seinem Gerät sogar Lebern reanimiert werden können, die bis zu eine Stunde nach dem Tod eines Patienten durch Herzstillstand entnommen wurden. „Die Zahl der verfügbaren Organe wäre riesig“, sagt er.

Eine Maßnahme von Larges Team dürfte jedoch

befremdlich wirken: In einigen Fällen haben die Mediziner das Herz noch im Körper der verstorbenen Patienten neu gestartet. Diese waren Opfer von Autounfällen oder eines Selbstmordversuchs. Sie hatten schwere Hirnschäden erlitten, waren aber nicht hirntot. Solche Patienten müssen meist künstlich beatmet werden und einige sterben kurze Zeit,

nachdem ihre Familien sich für das Abschalten der Lebenserhaltungssysteme entschieden haben.

Nach dem Kreislaufzusammenbruch und dem darauf folgenden Herzstillstand wartet Larges Team fünf Minuten. Anschließend bringt es das Herz zum Schlagen, indem es den Spender an eine künstliche Lunge anschließt: Das Gerät versorgt das Blut mit Sauerstoff und entzieht ihm das Kohlendioxid. Das Hirn koppeln sie von der Blutversorgung ab. Es kann sonst anschwellen. Dadurch steigt der Blutdruck massiv, was zum Versagen weiterer Organe führen kann.

Der Vorteil der ungewöhnlichen Prozedur: Wenn das Herz aktiv ist, lässt sich sein Zustand Large zufolge exakter überprüfen. Zudem werden Nieren und Leber weiter mit Blut versorgt, sodass auch diese als Spender-Organ zur Verfügung stehen. Nachdem die Herzen im Körper der Spender wieder schlugen, wurden sie entnommen und jeweils an das Transmedics-Gerät angeschlossen. Alle acht britischen Herzverpflanzungen waren erfolgreich.

Medizinethiker treibt allerdings die Frage um: Wenn sich ein Herz noch im Körper des Spenders wiederbeleben lässt, kann dieser dann wirklich als tot gelten? „Tot sind sie erst dann, wenn der Herzstillstand unwiderruflich ist“, sagt Ralf Stoecker, Professor für Praktische Philosophie an der Universität Bielefeld. „Wenn das Herz aber neu gestartet wird, wie kann man daran festhalten, dass der Patient tot war – auch wenn ihn niemand wiederbeleben wollte?“

Der Medizinethiker Robert Truog von der Harvard University sieht es etwas anders. „Meine Meinung ist, dass diese Spender zwar nicht tot sind“, sagt er. „Aber das spielt keine Rolle“ – sofern sie und ihre Familien vorher ihre Einwilligung für eine Spende gegeben haben. „Die Frage ist, ob ihnen Schaden zugefügt wird. Ich würde sagen, das ist nicht der Fall.“

ANTONIO REGALADO UND VERONIKA SZENTPÉTERY

Der neue Prototyp aus Bayern. Verschlüsselt von secunet.

Wer mit sensiblen Informationen arbeitet, kommt vorher zu uns. Wir beraten, konzeptionieren, implementieren und betreuen Sie rund um alle Fragen der IT-Sicherheit. So stellen wir sicher, dass die falschen Leute nur das wissen, was sie wissen dürfen: nichts. Und sorgen dafür, dass die richtigen Informationen nur die richtigen Personen erreichen.

Klingt unmöglich? Testen Sie uns!

www.secunet.com



secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland



MARTIN DÜRR,
Physiker am Forschungszentrum Jülich, hilft Atomkontrolleuren, Wischproben aus Anreicherungsanlagen auszuwerten.

INTERVIEW

» Spuren sind kaum zu vermeiden. «

TR: Wie können profane Tücher bei Atomkontrollen helfen?

Dürr: Die Inspekture der Internationalen Atomenergiebehörde IAEA können mit den trockenen Baumwolltüchern kleinste Spuren von Uran- oder Plutonium-Isotopen aufnehmen und aus der Analyse Schlüsse ziehen: ob etwa in einer Urananreicherungsanlage nur für zivile Zwecke oder auch für militärische angereichert wurde. Findet man nur niedrig angereichertes Uran, lässt sich mit einer gewissen Sicherheit sagen, dass in dieser Anlage kein Missbrauch stattgefunden hat. Eines der Uran-Isotope – U-235 – ist spaltbar und in hoher Konzentration waffenfähig. Bei der Anreicherung für zivile Anwendungen wie die Stromerzeugung in Kernkraftwerken ist es nicht so hoch konzentriert vorhanden.

Aber wie kommen die Isotope überhaupt aus den Maschinen heraus?

Es ist wie bei kriminaltechnischen Untersuchungen: Bestimmte Spuren sind kaum zu vermeiden. Es gibt immer winzige Lecks oder es werden Behälter

angeschlossen oder abmontiert, deshalb ist es eigentlich unvermeidbar, dass gasförmiges Uranhexafluorid entweicht und sich etwa an Rohren niederschlägt. In Atomkraftwerken sind keine abwischbaren Spuren zu erwarten, weil das nukleare Material – die Brennelemente – verschlossen ist.

Gehen wir nochmal zurück zu den Tüchern: Was genau passiert mit ihnen nach der Probenentnahme?

Es ist zunächst wie beim Doping: Die IAEA teilt das Material in A- und B-Proben und schickt sie an getrennte Labore. Dort wird entweder das gesamte Wischtuch chemisch aufgelöst, um nach Uran- oder Plutonium-Isotopen zu suchen. Oder es werden einzelne Partikel aus dem Tuch herausgelöst, zum Beispiel abgesaugt. Dann werden sie in einem neuen, sehr sensitiven Massenspektrometer untersucht. Und dafür haben wir sogenannte Referenzpartikel hergestellt.

Was genau sind Referenzpartikel?

Mit ihnen lässt sich prüfen, ob die

Massenspektrometer verlässliche Messergebnisse liefern. Massenspektrometer bestimmen ja die Masse von Urantomen und damit, um welche Isotope es sich handelt. Dafür müssen die Geräte kalibriert werden. Das ist so ähnlich, wie Waagen mit bekannten Gewichten geeicht werden, damit sie bei einem Kilo wirklich ein Kilo anzeigen.

Und wie stellt man solche winzigen Partikel mit definiertem Gewicht her?

Wir stellen zunächst aus einer Uran-Lösung mit einer bestimmten Konzentration Tröpfchen mit definierter Größe her. Nachdem das Lösemittel verdunstet ist, entstehen kleine, runde Partikel. Durch unsere Ausgangslösung können wir steuern, wie viele Uranatome in den Partikeln enthalten sind und welche Isotopenzusammensetzung sie haben. Diese Information geben wir dann an die Labore weiter. Damit können sie überprüfen, ob ihr Gerät richtig kalibriert ist und die richtigen Werte anzeigt.

INTERVIEW: V. SZENTPÉTERY

VERKEHR

Ampelphase auf dem Autodisplay

Wann springt die Ampel um? Lohnt es sich, den Motor abzustellen? Für diese Fragen hat das US-Startup Connected Signals eine App namens EnLighten vorgestellt. Sie zeigt dem Fahrer an, wie lange die aktuelle Ampelphase noch dauert. Anders als bei ähnlichen Projekten gibt es dabei keine direkte Kommunikation zwischen Ampel und Auto. Stattdessen bezieht die Software ihre Daten aus dem Verkehrsmanagementsystem, das die Ampeln steuert. Die Positionierung per GPS sagt ihr, vor welcher Ampel sie gerade steht.

Die Nutzung von EnLighten ist einfach: Ein grüner Pfeil signalisiert dem Fahrer, dass er mit der aktuellen Geschwindigkeit die Grünphase noch

erwischt. Bei einem roten Pfeil kann er den Wagen entspannt ausrollen lassen.

Noch komfortabler ist es, wenn die App nicht nur isoliert auf dem Smartphone läuft, sondern mit dem Auto verbunden ist. Dann erkennt sie unter anderem auch, ob ein Blinker gesetzt ist, und zeigt nur die zuständige Ampel an.

Das geht derzeit allerdings ausschließlich mit BMW-Fahrzeugen.

Im Rahmen eines Projekts des US-Verkehrsministeriums funktioniert die Technik bereits bei 2000 Ampeln in Portland, Eugene und Salt Lake City. Ob EnLighten nach Europa kommt, ist noch unklar.

BEN SCHWAN

Nur keinen Stress:
Die Ampel ist noch
28 Sekunden grün.



Foto: BMW

UMWELT

Unbemanntes Forschungsboot

Fischschwärme, Plastikmüll, Salzgehalt –

Biologen und Ozeanografen untersuchen viele Parameter, um den Zustand der Meere zu analysieren. Zusätzlich zum aufwendigen Einsatz von Forschungsschiffen und Satelliten könnte bald auch ein autarkes Roboterboot wichtige Daten liefern. Entwickelt vom britischen Unternehmen „ASV – Unmanned Marine Systems“ in Portchester, wird die Enduro-C drei Monate per Satellit gesteuert. Sie kann bis zu 6.500 Kilometer zurücklegen.

Derzeit testet das Unternehmen seine Einsatztauglichkeit in der keltischen See südlich von Irland zusammen mit dem britischen National Oceanography Centre. Neben der Analyse der Wasserqualität soll ein einfaches Sonarsystem Plankton- und Fischschwärme erkennen. Videokameras über Wasser liefern Daten zu Treibgut wie Plastikmüll sowie zu Anzahl und Verhalten der Tiere. Mikrofone zeichnen dazu etwa Rufe von Meeressäugern auf. Von der Güte der Daten wird es abhängen, ob solche Roboterboote künftig auf Expedition geschickt werden.

An Deck des gut vier Meter langen und mit Zuladung eine halbe Tonne schweren Katamarans liefern Solarzellen mit 1200 Watt und ein Windrad mit 720 Watt Strom für zwei Gleichstrom-Motoren, die Sensorelektronik und die Funktechnik. Ein Diesellgenerator als Notstromaggregat ergänzt die mobile Energieversorgung des bis zu sieben Knoten schnellen Boots. JAN OLIVER LÖFKEN

Das unbemannte Forschungsboot Enduro-C beim Test in der keltischen See.



Foto: ASC - unmanned marine systems

Machen Sie
Ihr Zuhause
smart
mit Somfy



 TaHoma®

Mit intelligenter Hausautomatisierung von Somfy steuern Sie Rollläden, Sonnenschutz, Tore und vieles mehr ganz bequem per iPad und Co. – auch von unterwegs.

www.somfy.de



somfy®

 Building happiness



sinkt der Preis von Auto-Akkus jeden Monat. Das hat der Trendforscher Lars Thomsen berechnet. Im gleichen Maße steigen laut Thomsen auch die Haltbarkeit und die Energiedichte.

MEDIZIN

Kleber für schwere Wunden



Polymer zum Verschließen stark blutender Wunden.

Stark blutende Wunden könnten künftig mit einem biologischen Polymergel verschlossen werden, das in die Wunde verabreicht diese in Sekunden fest verschließt. Entwickelt hat es der Jungunternehmer Joe Landolina, Gründer des US-Start-ups Suneris. Das bioverträgliche Gel besteht aus zwei algenbasierten Verbindungen. Bei Kontakt mit Blut polymeri-

sieren sie zu einem Material, an dessen Oberfläche positiv geladene Ionen sitzen. Dadurch zieht es Blutplättchen und rote Blutkörperchen rasch an, die außen negativ geladene Molekülgruppen tragen. Sie bleiben am Gel haften und bilden ein engmaschiges Netz. Dank des Polymers bindet dort das Gerinnungsprotein Fibrin schneller, so Entwicklungsleiter Omar Ahmad. Anders als bisherige chirurgische Kleber müssen die Komponenten nicht erst vermischt werden. Das Material härtet in etwa zehn Minuten aus. Es ist bioabbaubar, lässt sich aber auch nach der vollständigen Aushärtung wieder entfernen.

In Tierversuchen mit Schweinen verschloss das Gel nicht nur punktierte Gefäße, sondern auch komplett durchtrennte Oberschenkelarterien. Unter dem Namen Vetigel ist es für die Tiermedizin auf dem Markt. Am 1. November startet die Auslieferung, wegen der geringen Produktionskapazitäten vorerst nur im Nordosten der USA. Die Rezeptur für Menschen ist Ahmad zufolge ebenfalls fertig; Suneris arbeitet noch an größeren Applikatoren und plant die klinischen Versuche. Es will das Produkt in den nächsten anderthalb Jahren zur Zulassung anmelden. Zielmärkte sind die Notfallmedizin und das Militär. V. SZENTPÉTERY

ENERGIE

Strom aus dem Ozean



Meereswärme-Pilotkraftwerk auf Hawaii

Der Kraftwerkspark auf Hawaii ist seit wenigen Wochen um eine einzigartige Pilotanlage reicher. Auf dem Gelände des Natural Energy Laboratory in Keahole Point installierten Ingenieure des Unternehmens Makai Ocean Engineering ein Meereswärme-Pilotkraftwerk mit 100 Kilowatt elektrischer Leistung und schlossen es an das Stromnetz der Insel an.

Das Kraftwerk funktioniert ähnlich wie eine Wärmepumpe. Pumpen saugen warmes Oberflächenwasser aus dem Meer an. Über einen Wärmetauscher kann die Wärme auf ein Arbeitsmedium übertragen werden, etwa unter Hochdruck stehendes, flüssiges Ammoniak. Dieses verdampft. Der Dampf wird auf die Turbine eines kleinen Generators geleitet und erzeugt so Strom. Dann wird der Dampf mit bis zu fünf

Grad kaltem Meerwasser aus fast 1000 Meter Tiefe wieder verflüssigt und steht so für einen erneuten Kreislauf zur Verfügung.

Diese Kraftwerke erreichen nur Wirkungsgrade von maximal sechs Prozent, sind wegen ihres permanenten Betriebs aber grundlasttauglich. Derzeit wird ein größeres Meereswärme-Kraftwerk im küstennahen Gewässer mit bis zu 100 Megawatt Leistung geplant, für das die Entwickler Stromerzeugungskosten von etwa 17 Cent pro Kilowattstunde berechnet haben. Das wäre zwar etwa doppelt so teuer wie Windkraft, dafür würde der Strom ohne Schwankungen fließen. Da für einen effizienten Betrieb warmes Oberflächenwasser nötig ist, ist dieser Kraftwerkstyp in erster Linie für tropische Küstenregionen geeignet.

JAN OLIVER LÖFKEN

MEDIZIN

Virenpartikel statt Antibiotika

Forscher des Massachusetts Institute of Technology (MIT)

wollen der Antibiotika-Krise mit künstlichen Viren Herr werden. Ihre Arbeit baut auf der seit Jahrzehnten bekannten Phagentherapie auf. Dabei kommen sogenannte Bakteriophagen zum Einsatz: Viren, die selektiv nur bakterielle Erreger töten. Das Problem war bisher jedoch, dass deren massenhafte Auflösung zu einer tödlichen Blutvergiftung (Sepsis) führen kann. Die Forscher um James Collins konstruierten daher auf molekulargenetischem Weg künstliche Viruspartikel,

Illustration: Christine Daniloff und Jose-Luis Olivares/MIT.



sogenannte Phagemide. Diese schleusen einen kleinen DNA-Ring (Plasmid) mit ausgewählten Genen in die Bakterienzellen hinein. Er löst die Produktion von tödlich wirkenden Eiweißen aus. Die Zellwand der Bakterien bleibt intakt, eine Sepsisgefahr entsteht also nicht. Wie die Forscher im Fachjournal „Nano Letters“ schreiben, heilte ihre Therapie in Versuchen mit Mäusen, bei denen das Bakterium *Escherichia coli* eine Bauchfellentzündung verursacht hatte, 80 Prozent der Tiere. Nun wollen sie die Methode auf andere problematische Keime ausweiten. Das große Potenzial der Phagemide sehen die Wissenschaftler darin, erst mit Schnelltests den genauen Bakterienstamm zu ermitteln und dann das passende Phagemid zu verabreichen.

TOBIAS STOLZENBERG

ENERGIE

Brennstoffzelle fürs iPhone

Die britische Firma Intelligent Energy hat eine interne Brennstoffzelle für das iPhone 6 entwickelt. Wie die britische Zeitung „The Telegraph“ berichtet, brachten die Entwickler die Brennstoffe zusätzlich zu der Batterie in dem dünnen Gehäuse unter. Sie soll genug Strom liefern, um das Smartphone eine ganze Woche zu versorgen. Über die Durchführung der Kopfhörerbuchse sollen Wegwerfkartuschen die Brennstoffzelle mit wasserstoffhaltigem Pulver versorgen. Intelligent Energy geht davon aus, dass die Markteinführung des länger haltbaren iPhones noch ein paar Jahre dauere. Allerdings hinge das auch vom Partner ab. Gemeint ist Apple.

KARSTEN SCHÄFER



Startkapital für junge Technologieunternehmen

Der High-Tech Gründerfonds (HTGF) ist Deutschlands aktivster und größter Frühphaseninvestor. Wir finanzieren Ihr Technologie-Startup – von Cleantech und Robotik bis Wirkstoffentwicklung, von Chemie bis Software.

Nutzen Sie die Erfahrung und die umfangreichen Netzwerke unseres Teams mit seinem technologischen und betriebswirtschaftlichen Know-how.



High-Tech Gründerfonds

High-Tech Gründerfonds Management GmbH

Schlegelstraße 2 | 53113 Bonn

Telefon: +49 (0)228-82300-100

info@htgf.de

www.high-tech-gruenderfonds.de

/htgf.vc /htgf_



UMWELT

Den künftigen Lärm simulieren

Welchen Lärm verursacht

eine Straße, die noch gar nicht gebaut ist? Dieser Frage gehen Wissenschaftler der Forschungsorganisation Sintef aus Skandinavien nach. Zwar sieht die EU-„Umgebungslärmrichtlinie“ Lärmkarten für bereits vorhandene Straßen und geplante Projekte vor. Doch diese Karten zeigen lediglich die Lautstärke farblich codiert an. Wie der Lärm tatsächlich klingt, bleibt abstrakt. Deshalb haben die Forscher um Erlend Viggren ein Simulations-Tool entwickelt, das den künftigen Geräuschpegel an einer beliebigen Position hörbar macht.

Dazu nehmen sie zuerst die Geräusche einzelner Autos auf – jeweils an der vorderen und hinteren Stoßstange sowie bei 30, 50 und 80 Stundenkilometern. Dann baut das Sintef-Team mit einer Software ein Computermodell der geplanten Straße sowie der existierenden Umgebung einschließlich Vegetation. Platzieren sie einen Hörer virtuell in dieses Modell, können sie mit Filtern simulieren, wie Gebäude die Autogeräusche zurückwerfen und wie sie beim Hörer ankommen. Über Lautsprecher oder Kopfhörer können sich Nutzer dann einen Eindruck von der künftigen akustischen Landschaft machen. Die Software soll für die Straßenplanung genutzt werden.

JENNIFER LEPIES

ESSEN

Fruchtgummi aus dem 3D-Drucker



Einmal Oktopus süßsauer, bitte.

Foto: Katjes MCF

Wer Gummibärchen und

Lakritz-Kätzchen zwar lecker, aber langweilig findet, der kann im Katjes-Café in der Rosenthaler Straße in Berlin-Mitte neue Formen vernaschen. Ein eigens entwickelter 3D-Drucker erwärmt eine Spezialmischung und trägt sie schichtweise mit einer Düse auf. Über die genauen Zutaten verrät Katjes nicht mehr, als dass sie vegan, gluten- und laktosefrei seien und Pectin als Geliermittel enthalten.

3D-Drucker für Essen gibt es schon länger (siehe TR 7/2014, S. 50), aber das Katjes-Gerät ist nach Angaben des Unternehmens der „weltweit erste lebensmittelzertifizierte 3D-Drucker für Fruchtgummis“ – und zudem der

schnellste in seinem Segment: Für ein zehn Gramm schweres Fruchtgummi braucht er laut Katjes maximal fünf Minuten.

Bisher darf der Besucher lediglich zwischen zehn Formen sowie sieben Farben mit den entsprechenden Aromen wählen. Sie lassen sich auch im Mix auftragen und mit süßen oder sauren Verzierungen ergänzen. Künftig sollen aber weitere Optionen hinzukommen. Wer es noch individueller mag, kann auch Grüße auf Fruchtgummi-Karten drucken lassen.

GREGOR HONSEL

INFOTECH

Surfen mit Alibi

Internetnutzer haben keinerlei Einfluss darauf, ob ihre Datenpakete durch Länder wandern, in denen sie möglicherweise ausspioniert werden. Computerwissenschaftler der University of Maryland geben Nutzern nun mehr Kontrolle darüber. Ihre Verfahren namens „Alibi Routing“ erlaubt es, bestimmte Länder auszuschließen. Die Technik basiert auf dem Peer-to-Peer-Prinzip: Rechner in aller Welt, auf denen die entsprechende Software läuft, reichen die Daten untereinander weiter. Um sicherzustellen, dass die Pakete nicht durch verbotene Länder wandern, wählt die Software stets Knotenpunkte, die weit genug von der Verbotszone entfernt sind. Würde der Datenverkehr dann trotzdem noch durch unerwünschte Gebiete laufen, ergäbe sich dadurch eine erkennbare Verzögerung. Derzeit ist die Technik noch im Prototypstadium.

BEN SCHWAN

NEUER REKORD

Supraleitung bei minus 70 Grad entdeckt

Foto: A. P. Drozdov et al./Nature, DOI: 10.1038/nature14964

In der runden Presszelle wird unter hohem Druck aus Schwefelwasserstoffgas ein Metall.



Kupferoxid-Verbindungen zählen zu den besten Supraleitern. In ersten Kabeln leiten sie bereits Strom ohne Widerstand. Doch sie müssen mit flüssigem Stickstoff mindestens auf minus 139 Grad Celsius abgekühlt werden. Jetzt haben Mikhail Erements und Kollegen vom Max-Planck-Institut für Chemie und der Uni Mainz eine Schwefelwasserstoff-Verbindung geschaffen, die schon bei minus 70 Grad in den supraleitenden Zustand überging. Dazu

übten die Forscher mit einer Diamantpresszelle starken Druck auf Schwefelwasserstoffgas aus. Bei 96 Gigapascal wandelte es sich zu einem Metall. Tiefgeköhlt auf nur minus 70 Grad konnten die Forscher klare Zeichen für einen supraleitenden Stromtransport erkennen.

Sie gehen davon aus, dass sich ein supraleitendes Schwefelhydrid aus einem Schwefel- und drei Wasserstoffatomen gebildet hat. Zwar lässt sich daraus wegen der hohen Drücke kein technisch nutzbares Kabel fertigen. „Diese Entdeckung macht trotzdem Hoffnung auf Supraleitung bei Raumtemperatur mit anderen wasserstoffhaltigen Materialien“, schreiben die Forscher in „Nature“. J. O. LÖFKEN

INFOTECH

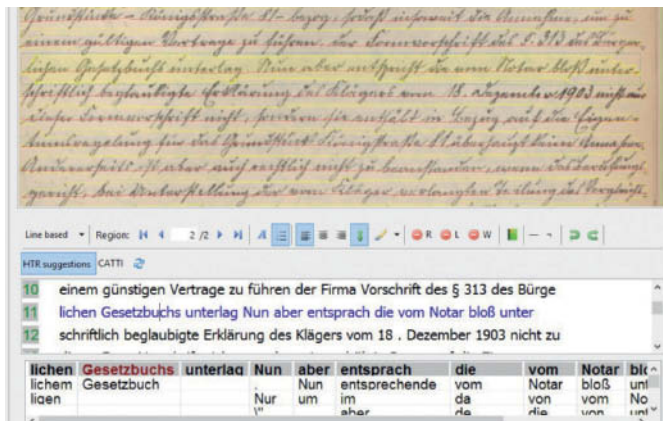
Computer liest historische Handschriften

Forscher der Universität Innsbruck arbeiten an einer Plattform zur Erkennung von historischen Handschriften. Schon bald sollen Archive, aber auch die breite Öffentlichkeit Dokumente unserer Vorfahren leichter lesen können. Auch eine App zum mobilen Einscannen von Handschriften ist geplant. Das Projekt soll 2016 starten.

Ziel der Forscher ist es, die Software mit dem Namen Transkribus durch möglichst breiten Einsatz zu trainieren und dadurch die Erkennungsraten von heute

70 bis 80 Prozent laufend weiter zu verbessern. Den Transkribus zugrunde liegenden Algorithmus haben Forscher aus Valencia und Athen geschrieben. Insgesamt sind 13 europäische Länder an dem Projekt beteiligt.

KARSTEN SCHÄFER



Die Schrifterkennung Transkribus erfasst historische Handschriften und macht sie in Druckschrift lesbar.

Internationale Fachmesse
Ideen · Erfindungen · Neuheiten

iENA In Kombination mit:
START MESSE
Gründung
Finanzierung
Nachfolge
Franchising
31.10.+1.11.
MESSE NÜRNBERG

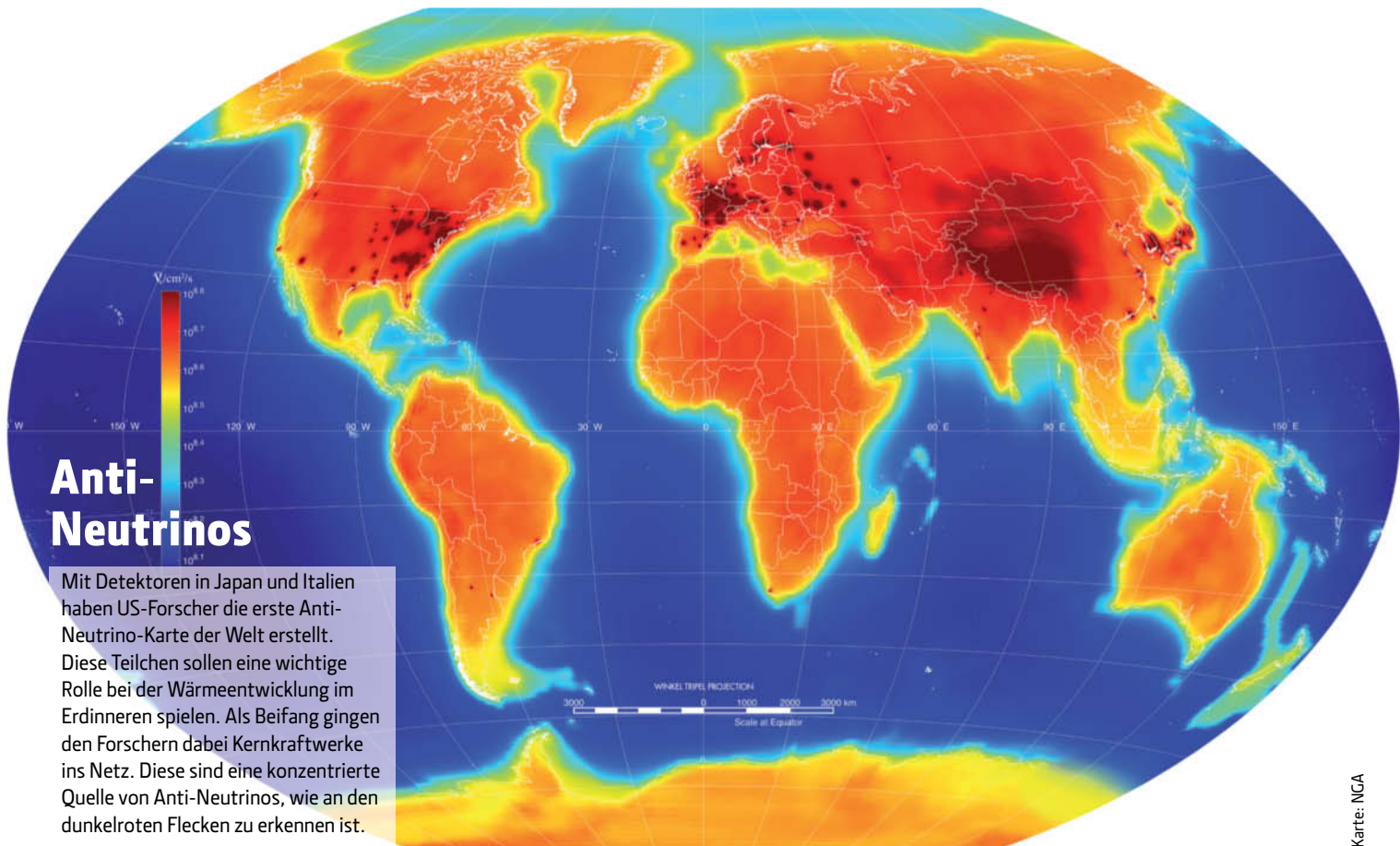
2015
29. Okt. – 1. Nov.



- **Neue Ideen für den Markt.** Die iENA 2015 Nürnberg ist der internationale Markt für Ideen, Erfindungen und Neuheiten.
- **Wichtig für alle,** die Erfindungen und Neuheiten verwerten und Top-Kontakte zu Erfindern suchen.
- **iENA-Symposium** „Mit der Idee zum Erfolg“, Samstag, 31.10., 10–12:30 Uhr (Teilnahme im iENA-Eintritt enthalten)
- **Innovationsseminar:** „Strategien des Innovations-Managements“, Freitag, 30.10., 10–16 Uhr (Teilnahme im iENA-Eintritt enthalten)
- **Fachberatung und Information**
Messe Nürnberg · Halle 12

In Kooperation mit: **PSI** **IFIA** **Consumenten**
Veranstalter/Organisation
AFAG
Messen und Ausstellungen GmbH
09 11-9 88 33-570
iena@afag.de · www.iena.de

Screenshot: Universität Innsbruck



Anti-Neutrinos

Mit Detektoren in Japan und Italien haben US-Forscher die erste Anti-Neutrino-Karte der Welt erstellt. Diese Teilchen sollen eine wichtige Rolle bei der Wärmeentwicklung im Erdinneren spielen. Als Beifang gingen den Forschern dabei Kernkraftwerke ins Netz. Diese sind eine konzentrierte Quelle von Anti-Neutrinos, wie an den dunkelroten Flecken zu erkennen ist.

Karte: NCA

INFOTECH Sicher dank Sound

Ein Passwort mag noch so lang und kompliziert sein – fällt es einem Hacker in die Hände, hat der freie Fahrt. Bei wichtigen Anwendungen wie etwa Online-Überweisungen ist deshalb

die sogenannte Zwei-Faktoren-Authentifizierung Standard. Das heißt: Neben dem Passwort gibt es noch ein weiteres Sicherheitsmerkmal, etwa eine per SMS an das Handy des Nutzers gesendete Transaktionsnummer.

Anzeige



Softwareinnovationen für
Energie-, Arbeits- und Rohstoffeffizienz

Sonderlich bequem ist das allerdings nicht.

Ein Forscherteam der ETH Zürich hat die Zwei-Faktoren-Authentifizierung deshalb radikal vereinfacht. Dazu nutzt es die Mikrofone vom PC und vom Handy des Nutzers. Sie nehmen während des Einloggens die Umgebungsgeräusche auf. Empfangen beide Geräte dieselben Geräusche, müssen sie folglich am gleichen Ort sein. Und derjenige, der über den Rechner ein Passwort eingibt, hat auch Zugriff auf das angemeldete Handy. Hätte ein Hacker einfach nur ein Passwort erbeutet, wäre das nicht der Fall.

Das System soll nach Angaben der Forscher sogar dann funktionieren, wenn das Handy im Rucksack steckt. Nun arbeiten sie daran, ihr Verfahren marktreif zu machen.

BEN SCHWAN

MATERIALIEN

Quallen-Protein für Lampen

Wissenschaftler der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) haben weiße Leuchtdioden entwickelt, die fluoreszierende Proteine enthalten. Die Proteine sollen eine deutlich preisgünstigere und nachhaltigere Produktion ermöglichen.

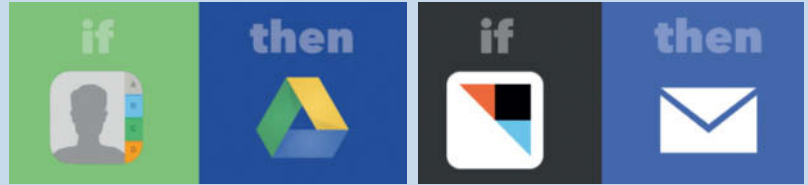
Bislang bestehen weiße LEDs in der Regel aus einem blau oder ultraviolett leuchtenden Kern, der mit einer dünnen Schicht überzogen wird. Diese Schicht, die unter anderem sogenannte Seltene Erden enthält, wandelt das Licht des Kerns in weißes Licht um. Die Produktion ist allerdings vergleichsweise teuer – außerdem sind die Seltenen Erden nicht unbegrenzt verfügbar.

Das Team um Uwe Sonnewald verwendete nun eine organische Schicht, die grün, rot und blau fluoreszierende Proteine enthält. Ursprünglich stammt das grüne Protein von Quallen – rot und blau wurden von anderen Forschungsgruppen durch chemische Veränderungen daraus abgeleitet.

Um die Proteine auf die LED aufbringen zu können, entwickelten die Wissenschaftler ein Gel aus einer konzentrierten Protein-Lösung und einer Polymischung. Durch Vakuumtrocknung verwandelt sich das Gel in ein gummiartiges Material, das „überraschenderweise die Proteine massiv stabilisiert“, sagt Sonnewald. Die Laufzeit der hybriden LEDs beträgt bislang zwar nur einige hundert Stunden. Da das System aber noch nicht optimiert ist, sind die Forscher optimistisch, bald „deutlich längere Laufzeiten“ zu erreichen. WOLFGANG STIELER



IF Wenn dies passiert, tu jenes

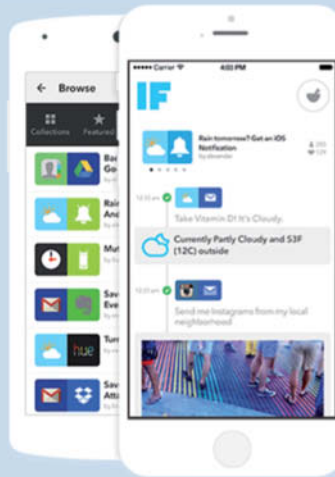


Früher habe ich abends immer vergessen, mein Handy leise zu stellen, um nicht vom Bimmeln verschiedener Benachrichtigungen geweckt zu werden. Erinnernte ich mich einmal, vergaß ich am nächsten Morgen wieder, es lautzustellen, und verpasste Anrufe. Warum kann das Handy das nicht automatisch machen? Die äußerst praktische App „If“ ermöglicht es. Sie verknüpft verschiedene Handy-Funktionen oder Apps miteinander, und zwar nach der einfachen Regel: „Wenn dies passiert, dann tu jenes“. In meinem Fall: Wenn es 22 Uhr ist, drehe die Lautstärke runter; und um 8 Uhr drehe sie wieder hoch. „If“ nennt diese Automatisierungen „Rezepte“

und bietet eine ganze Reihe voreingestellter Regeln an, nach Themen geordnet. Zudem lässt es Nutzer selbst welche erstellen und an andere Nutzer posten.

Damit kann man etwa jedes Foto zur Sicherung in die Dropbox hochladen lassen. Oder bei einem verpassten Anruf den Namen des Anrufers automatisch für einen Rückruf bei der „Todoist“-App vormerken. „If“ erlaubt auch das Einbinden von Apps für externe Geräte wie den Nest-Rauchdetektor oder die Philips-Lampe Hue. Das Schmökern in den Rezepten lohnt sich. Die kostenlose App gibt es für Android und iOS.

VERONIKA SZENTPÉTERY



Anzeige





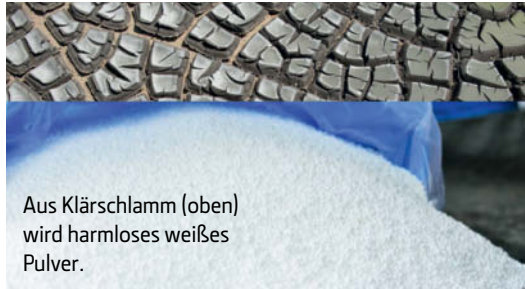
UMWELT

Dünger aus Klärschlamm

Klärschlamm enthält viel Phosphat und ist deshalb ein wertvoller Dünger. Allerdings gelangen mit ihm auch giftige Schwermetalle auf die Felder. Andrea Kruse von der Uni Hohenheim hat nun gemeinsam mit der Schweizer Biotech-Firma AVA-CO2 ein Verfahren entwickelt, um beide zu trennen. Dazu erhitzt sie den Schlamm zwei Stunden lang auf 200 Grad („Hydrothermale Carbonisierung“). Dabei entsteht eine Masse, die kleine Bröckchen aus Biokohle enthält. Anschließend kocht Kruse die Masse mit Säure auf und trennt die Kohle ab. Getrocknet und mit Magnesiumsalz versehen, entsteht aus dem Rest das weiße, körnige Mineral Struvit (Magnesium-Ammonium-Phosphat). Es enthält noch rund 80 Prozent des ursprünglichen Phosphats und kann gut von den Pflanzen aufgenommen werden.

Die Schwermetalle bleiben in der Biokohle. Sie hat einen höheren Heizwert als Klärschlamm und lässt sich deshalb gut verbrennen. Mit der Asche kann man die Giftstoffe dann relativ einfach entsorgen. Derzeit optimiert Kruse das Verfahren noch im Labor. Später soll die Produktion ausgeweitet werden.

GREGOR HONSEL



Aus Klärschlamm (oben) wird harmloses weißes Pulver.

MILITÄR

Laser gegen Drohnen

Boeing hat ein mobiles Lasersystem zum Abschuss von kleinen Drohnen entwickelt. Ende August hat der Konzern damit nach eigenen Angaben auf einem Übungsgelände in Kalifornien eine nicht näher beschriebene unbemannte Drohne im freien Flug abgeschossen.

Neben Boeing entwickeln auch andere Rüstungsschmieden Laserwaffen, darunter Lockheed Martin, MBDA und Rheinmetall Defense. Nahezu all diese Waffen sind Faserlaser. Sie enthalten eine lange, aufgerollte Glasfaser. In deren Mantel befinden sich Metallatome, die von Diodenlasern in den angeregten Zustand versetzt werden. Im Laserblitz wird die gespeicherte Energie dann auf einen Schlag entladen.

Boeing arbeitet seit Jahren auch an einer Laserwaffe, die Raketen abschießen soll. Die benötigt für ihre 10-Kilowatt Leistung allerdings einen Lastwagen als Unterbau.

Der neue „ultraportable“ Laser dagegen arbeitet mit zwei Kilowatt und besteht aus vier koffergroßen Modulen, die von zwei Männern getragen werden können. Die Waffenfabriken bewerben die Geräte als besonders kostengünstig, da ein Schuss sehr viel billiger ist als eine Rakete oder Granate. Bei Regen oder Nebel funktionieren die Strahlenwaffen allerdings nicht gut, da Wasserdampf ihre Infrarotstrahlung absorbiert.

WOLFGANG STIELER



Fast wie bei Star Wars: Laserkanone von Boeing.

watchlist politik

BUND GEGEN GENMAIS

Bundesagrarminister Christian Schmidt (CSU) hat die Agrarkonzerne aufgefordert, in Deutschland keinen Genmais mehr zu vermarkten – selbst wenn dieser in der EU zugelassen ist. Weigern sich die Konzerne und erlassen die Bundesländer keine eigenen Gesetze, will Schmidt den Anbau per Bundesgesetz verbieten.

BRÜSSEL GEGEN BRAUNKOHLE

Bundeswirtschaftsminister Sigmar Gabriel (SPD) hat mit den Energieversorgern mühsam einen Kompromiss ausgehandelt, wonach alte Braunkohlekraftwerke gegen eine Entschädigung als Reserve in Betrieb bleiben dürfen. Nach einem Bericht der „Frankfurter Allgemeinen“ droht dieser Kompromiss nun an der EU-Kommission zu scheitern, weil sie dies als unerlaubte Beihilfe sieht.

BUNDESWEHR GEGEN HACKER

Bisher haben alle Truppenteile der Bundeswehr – Heer, Luftwaffe und Marine – ihre eigenen Cyberwar-Abteilungen. Nun will Bundesverteidigungsministerin Ursula von der Leyen (CDU) die Abteilungen zu einem eigenen, gleichgestellten Truppenteil zusammenlegen. Das berichtet die „Süddeutsche Zeitung“.

EU-KOMMISSION GEGEN GEO-BLOCKING

Die EU-Kommission hat das sogenannte Geo-Blocking ins Visier genommen. Dieses Verfahren erlaubt es Medienunternehmen, Filme oder Fernsehsendungen nur in bestimmten Ländern auszuspielen und so für jedes Sendegebiet einzelne Lizenzen zu verkaufen (siehe TR 6/2015, S. 84). Mit einer öffentlichen Konsultation will die Kommission nun den ersten Schritt zu einem einheitlichen, europaweiten Markt machen.

Foto: Hannes Grobe/Clipdealer/Wikimedia

Foto: Boeing

WELCHER POPSTAR TRUG HANDSCHUHE MIT GLITZERSTEINEN?

ZU EINFACH? GUT, WELCHER ERFINDER ENTWICKELTE DIE BIONISCHE HAND?



#WHYISIT

Wie kommt es, dass wir jedes kleine Detail aus dem Leben eines Popstars kennen, aber nichts über den schottischen Ingenieur wissen, der Prothesen entwickelt, die fast so gut funktionieren wie echte Hände? Ist es nicht an der Zeit, die Menschen zu beachten, die mit ihren Erfindungen die Welt verbessern? Menschen wie David Gow, dessen bahnbrechende Prothesentechnik Tausenden Menschen mit Behinderung mehr Mobilität und Freiheit schenkt. **Feiern wir die Heroes of Innovation!**

arrow.com/whysisit

ARROW



am markt

AUTO

Tesla Model X reservierbar

Es ist so weit. Das lang erwartete und schon oft verschobene Elektro-SUV aus dem Hause Tesla Motors lässt sich ab sofort reservieren. Erste Auslieferungen des Tesla Model X sollen Anfang nächsten Jahres erfolgen. Die Reservierung kann man über die Website von Tesla Motors tätigen, sie wird mit einer Anzahlung von 4000 Euro abgeschlossen.

Anschließend erhält man Zugriff auf den Konfigurator und kann verschiedene Ausstattungen des optionalen Siebensitzers ausprobieren.

Sämtliche Preise und Leistungsdaten sind allerdings noch unverbindlich.

Die sogenannte Signature-Edition des Model X soll schon bald für 132 000 Dollar erhältlich sein. Sie wird zum

Verkaufsstart wohl eine Batterie mit einer Kapazität von 90 Kilowatt-

stunden haben, die dem Allrader eine Reichweite von an die 400 Kilometer bescheren soll.

Dabei sorgen zwei Elektromotoren für Vortrieb, einer an der Vorderachse mit 259 PS und einer an der Hinterachse mit 503 PS. Der Spurt von 0 auf 100 km/h soll damit in 3,8 Sekunden gelingen.

Bei 250 Stundenkilometern macht die Leistungselektronik dann Schluss.



PRODUKT: Model X **HERSTELLER:** Tesla Motors **PREIS:** 132 000 Dollar (Signature Edition)

LINK: <https://my.teslamotors.com/own>



WEARABLES

Steampunk fürs Handgelenk

Das Nerd-Kaufhaus Thinkgeek hat mit der Tesla Watch eine Armbanduhr im Angebot, die aus einer futuristisch-viktorianischen Zeit zu stammen scheint. Die Sekundenanzeige neben dem Ziffernblatt könnte auch ein zu klein geratenes Manometer eines Dampfventils sein. Zwei abschaltbare rote Leuchtdioden stecken stilecht in Vakuumröhren. Das (elektronische) Uhrwerk selbst stammt aus Japan; ein mitgelieferter Schlüssel zum Aufziehen ist nur Show. Aber Achtung: Die Uhr benötigt insgesamt drei Kleinbatterien für Hauptzeit, Sekunden und LEDs. Ein Lederarmband liegt bei.

PRODUKT: Tesla Watch **HERSTELLER:** Thinkgeek **PREIS:** 60 Dollar

LINK: www.thinkgeek.com/product/imnl

SMART HOME

Der Garten wird digital

Gardena hat eine ganze Reihe von Gartengeräten vorgestellt, die mit der Cloud verbunden sind und sich per App steuern lassen. Ein Sensor erfasst etwa die Feuchtigkeit und Sonneneinstrahlung bei einer Pflanze (120 Euro). Ist es zu trocken, schafft ein digital steuerbares Bewässerungssystem namens „Smart Water Control“ Abhilfe (170 Euro). „Sileno“ und „Sileno+“ (1600 bis 1850 Euro) sind autonome Rasenmäher, die sich ebenfalls in das Smart-Garden-System einbinden lassen und sich dann auf Bewässerungszyklen einstellen. Der Sileno+ kann zudem die Mähfrequenz automatisch an das Graswachstum anpassen.



Damit die Geräte zusammenspielen, muss allerdings noch ein sogenanntes Gateway her (250 Euro). Die einzelnen Bestandteile sollen im ersten Quartal 2016 auf den Markt kommen.

Gardena plant auch den Verkauf von Paketen aus mehreren Produkten. Die App gibt es zunächst nur für iOS, eine Android-Version soll folgen.

PRODUKT: Smart System **HERSTELLER:** Gardena
PREIS: 120 bis 1850 Euro **LINK:** goo.gl/8Fxf9H

OUTDOOR

Vollmöbliertes Zelt

Zelt, Schlafsack und Iso-Matte in einem bietet das All-in-one-Schlafsystem des Schweizer Start-ups Polarmond. Je nach Variante wiegt der komplette Unterschlupf 3,9 bis 5,2 Kilogramm. Dazu gibt es noch eine kompaktere Biwak-Version. Die Außenhaut besteht aus einem wasserdichten, aber atmungsaktiven Material. Der direkte Einbau von Schlafsack und Unterlage soll nicht nur den Aufbau bequemer, sondern die Schlafgelegenheit auch wärmer machen. Zweistellige Minustemperaturen sollen sich laut Hersteller bequem überstehen lassen. Preise nennt Polarmond derzeit noch nicht. Im Handel sein sollen die Zelte im Frühjahr 2016.

PRODUKT: All-in-one-Zelt **HERSTELLER:** Polarmond **PREIS:** noch unklar
LINK: www.polarmond.ch



FREIZEIT

Aufrechter Fahrradständer

Wer seinen Drahtesel – etwa aus Angst vor Dieben – in die Wohnung mitnimmt, kennt das Problem: Das Zweirad frisst im Flur viel Platz. Aufrecht wäre es deutlich platzsparender, doch dafür benötigt man normalerweise eine fest montierte Aufhängung. Eine Alternative ist der Upright Bike Stand von Hammacher Schlemmer. Der Ständer aus robustem Kunststoff nimmt 12 bis 29 Zoll große Hinterräder auf, während eine Stange den Sattelbereich stützt. Speichen oder Schaltung werden nicht berührt, sodass sie auch nicht beschädigt werden können. Saugnäpfe halten den Ständer am Boden, Werkzeuge zum Aufbau benötigt man nicht. Im Sockel ist noch Platz für Fahrradzubehör. Stilvoll ist er allerdings nicht.

PRODUKT: Upright Bike Stand **HERSTELLER:** Hammacher Schlemmer
PREIS: 120 Dollar **LINK:** goo.gl/dGRwbT



FOTOGRAFIE

Infrarot für Profis

Von außen sieht die Fujifilm X-T1 IR aus wie eine normale Spiegelreflexkamera. Doch im Inneren befindet sich ein Bildsensor, der für das menschliche Auge unsichtbares Licht einfangen kann. Er erfasst Wellenlängen von 380 bis 1000 nm – reicht also sowohl in den ultravioletten als auch in den infraroten Bereich hinein. Der menschliche Sehbereich liegt zwischen 390 und 700 nm. Kriminalisten können damit etwa am Tatort unterschiedliche Temperaturen erfassen – und so feststellen, ob ein Täter einen Gegenstand kürzlich noch angefasst hat. Hobby-Astronomen oder Bildkünstlern verschafft die Infrarot-Fotografie interessante Bildeffekte, da sie Dinge sichtbar macht, die das menschliche Auge nicht wahrnimmt. Ganz günstig ist der Spaß allerdings nicht: Für das kleine Extra an Lichtwellenlängen verlangt Fujitsu rund 400 Dollar Aufpreis gegenüber der normalen X-T1, die weiterhin verkauft wird.

PRODUKT: X-T1 IR **HERSTELLER:** Fujifilm
PREIS: 1700 Dollar **LINK:** goo.gl/mPuRH9



FAHRRAD

500-Watt-Motor zum Nachrüsten

Der Schweizer Anbieter Maxon hat einen Radnaben-Motor zum Nachrüsten vorgestellt. Er leistet 500 Watt, wiegt 3,5 Kilogramm und hat ein maximales Drehmoment von 50 Newtonmetern. Damit kann er nach Angaben des Herstellers einen 80-Kilogramm-Fahrer in drei Sekunden von 0 auf 30 km/h beschleunigen – oder ihn in einer halben Stunde 1000 Höhenmeter erklettern lassen. Der Akku fasst 360 Wattstunden, wird am Rahmen verschraubt und soll eine maximale Reichweite von 100 Kilometern erlauben. Preisgünstig ist der Motor, der zunächst nur direkt in der Schweiz geordert werden kann, allerdings nicht: Er kostet 2800 Franken (2550 Euro). Unterstützt werden Räder mit Einbaubreiten zwischen 135 und 142 mm. Der Radhersteller Ibox will ihn demnächst ab Werk in Räder einbauen, die ab 5000 Franken (4550 Euro) verkauft werden. Nach deutschem Recht sind Räder mit mehr als 250 Watt allerdings nicht mehr zulassungsfrei – sie erfordern Kennzeichen und Führerschein.

PRODUKT: Bikedrive **HERSTELLER:** Maxon **PREIS:** ab 2800 Franken
LINK: www.maxonbikedrive.com



REIFEN

Keine Luft, kein Problem

Seit John Boyd Dunlop Ende des 19. Jahrhunderts luftgefüllten Pneus zum Durchbruch verhalf, gehören Reifenpannen zum Alltag. Michelin hat die Druckluft bei seinen Tweel-Reifen nun wegrationalisiert. Stattdessen verbinden Polyurethan-Lamellen die Lauffläche mit der Nabe. Ende 2014 hat Michelin in South Carolina eine eigene Fabrik für diese Reifen eröffnet. Sie sollen laut Michelin ebenso komfortabel sein wie klassische Pneus, aber zwei- bis dreimal so lange halten. Außerdem seien sie absolut pannensicher und wartungsfrei, da kein Luftdruck mehr kontrolliert werden muss. Zum Einsatz kommen sollen sie vor allem beim Bau und in der Landwirtschaft. Zum einen kosten dort Ausfallzeiten bares Geld, zum anderen sind die Reifen nur für 25 km/h zugelassen. Bisher gibt es sie nur für zwei Fahrzeuge: einen kleinen Radlader sowie die Rasenmäher der ZTrak-900-Serie von John Deere.

PRODUKT: Tweel Turf **HERSTELLER:** Michelin
PREIS: 474,50 Dollar/Stück **LINK:** www.michelintweel.com





AUSPROBIERT AM RAD DREHEN

Das Varibike wird parallel mit Händen und Füßen angetrieben. Im Vergleich zum normalen Fahrrad ist man deutlich schneller unterwegs – und trainiert den ganzen Körper.

Radfahren stärkt nicht gerade den ganzen Körper. Zwar ist die gelenkschonende Tretbewegung gut für die Ausdauer, aber genau genommen trainiert man nur die Beine. Beim „Varibike“ dagegen treten die Füße in die Pedale, die Hände drehen eine Kurbel – gemeinsam treiben sie das Hinterrad an.

Schnell zeigt sich allerdings, dass das Radeln mit allen Vieren nicht ganz einfach ist. Das Varibike hat zwar einen Lenker, im Handmodus sind die Hände aber an der Kurbel – und die ist im Rahmen gelagert, nicht in der Gabel. Lenken muss ich das Rad dann über Gewichtsverlagerung, was anfangs Mut braucht, nach ein wenig Übung aber verblüffend gut funktioniert. Denn beim Varibike sorgen die nach hinten gekippte Lenkachse und ein Gummi-Lenkungsdämpfer dafür, dass das Vorderrad stets in der Spur bleibt.

Ein paar Runden Eingewöhnung unter fachkundiger Anleitung vom Erfinder sind daher durchaus ratsam – dann geht es allein um die Hamburger Alster. Varibiken sieht zwar schräg aus, macht aber mordsmäßig Spaß. Dass „Vari“ für Variation steht, merke ich prompt. Denn ich kann das Rad nicht nur mit den Füßen antreiben, ich kann beide Arme synchron bewegen oder dank der Freilaufkurbeln versetzt, ich kann nur den linken oder nur den rechten Arm benutzen oder alles zusammen – dann beschleunigt man gefühlt auf Sportwagenniveau. Das surfähnliche Gefühl bei Kurvenfahrten ist grandios. Um bremsen zu können, muss ich allerdings bei voller Fahrt von der Kurbel auf den Lenker umgreifen. Das ist recht gewöhnungsbedürftig, kann einen schon



mal ins Schlingern bringen und ist bei einer Notbremsung nicht ganz ungefährlich. Immerhin: Das alles fördert die Koordination ungemein, der ganze Körper ist in Bewegung. Kurzum: Varibiken ist mit dem gewöhnlichen Radeln in etwa so vergleichbar wie Freeclimben mit Spazierengehen.

Brandneu ist das „Full-Body-Biken“ zwar nicht. Weltweit gibt es bereits eine gute Handvoll Hersteller solcher Spezialräder. Man merkt

diesem Varibike aber an, dass versierte Maschinenbauer und begeisterte Sportler am Werk waren: Alles ist solide verarbeitet und absolut durchdacht, was bei einem sportlichen Preis von 4999 Euro aber ohnehin selbstverständlich sein sollte. Der Aluminiumrahmen ist made in Germany, die Schweißnähte sind sauber verputzt und die fertigen Rahmen pulverbeschichtet. Dass sie stabil sind, hat das Prüflabor „Velotech“ in Schweinfurt bestätigt.

SCHALTUNG: Je nach Kundenwunsch von Shimano XT bis zur Rohloff-Getriebebox **GEWICHT:** 15 Kilogramm **VARIANTEN:** Erhältlich als Straßen-, Gelände-, Tandem- und Indoorversion (Hometrainer)
PREIS: ab 4999 Euro **LINK:** www.varibike.com



DANIEL HAUTMANN, freier Journalist, interessiert sich besonders für Technologien, die Fortschritt und Nachhaltigkeit verbinden.



Johann Gevers
ist Gründer der
Monetas AG –
und wie viele
in der Szene
hin- und
hergerissen
zwischen
Prinzipien und
Pragmatismus.

Von Punk zu Bank

Die **Anarcho-Währung Bitcoin** war als Frontalangriff auf das Bankensystem gedacht. Nun könnte sie sich tatsächlich daranmachen, den Finanzmarkt zu revolutionieren – wenn auch ganz anders als geplant. Eine Geschichte über Glücksritter, Finanzjongleure – und die Zukunft des Geldes.

VON ULF J. FROITZHEIM / MITARBEIT: GREGOR HONSEL

Dies ist eine Geschichte von mysteriösen Start-ups ohne Adresse, von selbst gedrucktem Geld, von einem 21-jährigen Mathegenie, das die Banken auf den Kopf stellen will, von einem Gründer, der sein Smartphone trägt wie die Cops in Krimis ihre Pistole – und von Geldgebern, die Millionen zahlen, um in dieser Szene dabei zu sein. Dies ist eine Geschichte über Bitcoin und darüber, wie eine oft tot geglaubte Idee das Finanzsystem verändern könnte.

Fangen wir am besten bei Blockstream an: Die Liste der Investoren liest sich wie ein Who's who des Silicon Valleys: Reid Hoffman und Max Levchin (PayPal; LinkedIn, Yelp), Vinod Khosla und Eric Schmidt (Sun Microsystems; Google), Jerry Yang (Yahoo) und Ray Ozzie (Lotus Notes, Microsoft) sowie der ehemalige Karstadt-Abenteurer Nicolas Berggruen. Sie legten opulente 21 Millionen Dollar Startkapital zusammen. Doch wo genau der Firmensitz ist, lässt sich kaum herausfinden. Spuren führen nach Montreal, enden dort aber in einer Anwaltskanzlei und einer UPS-Filiale. Existiert das Start-up nur in der Cloud, als lose Kooperation verstreuter Einzelgänger?

Das würde passen. Blockstream speichert Geschäftsvorgänge mit einer auf Bitcoin aufsetzenden Technik. Und in der Bitcoin-Szene sind Freiheit, Dezentralität und Anonymität Fixpunkte im Wertesystem. Selbst über den Bitcoin-Erfinder Satoshi Nakamoto ist praktisch nichts bekannt. Gewiss ist nur, dass er ein völlig neues Geldsystem schaffen wollte. Unmittelbar nach dem Crash

der Investmentbank Lehman Brothers stellte er die Idee für ein offenes Peer-to-Peer-Netz online, dessen Teilnehmer sich neue „Münzen“ verdienen können, indem sie sich gegenseitig auf die Finger schauen. Die Idee faszinierte Netzaktivisten verschiedenster Couleur – von libertären Hardlinern über Occupy-Autonome und Cypherpunks bis zu Verschwörungstheoretikern.

Nakamotos Prinzip hieß „trustlessness“: Traue keinen Menschen oder Institutionen, sondern nur Open-Source-Algorithmen und der Crowd. Damit war theoretisch der Weg frei für eine globale Währung unter Umgehung der Banken, die sich damals in eine tiefe Vertrauenskrise manövriert hatten.

Nun sind die Geldinstitute allerdings dabei, den Spieß umzudrehen: Sie reizt nicht so sehr das Kunstgeld an sich, sondern das dahinterliegende „Blockchain“-Prinzip – ein dezentrales Kassenbuch aus einer endlosen Kette von Datenblöcken. Da sie nicht nur Einnahmen und Ausgaben protokollieren können, sondern jeden beliebigen Geschäftsvorgang, eignen sie sich als Universalwerkzeug für Finanzdienstleistungen und Beurkundungen aller Art. So sondieren bereits Deutsche Bank, UBS, ABN Amro und Citibank die Chancen und Risiken. Mitte September gaben neun der weltgrößten Banken die Gründung einer Partnerschaft bekannt, um einheitliche Protokolle und Industriestandards für Blockchain-basiertes Banking zu entwickeln – darunter Barclays, Credit Suisse und JPMorgan. Bitcoins als Währung mögen seit

ihrem Allzeithoch mehr als 80 Prozent an Wert verloren haben – die Firmen, die sich der Bitcoin-Technologie bedienen, bekamen allein 2015 mehr als 400 Millionen Dollar an Risikokapital.

„Die Blockchain ist die entscheidende Innovation“, bestätigt Matthias Kröner. Der Chef der kleinen Münchener Fidor Bank hat sich einen Namen als innovationsfreudiger Banker gemacht. Gemeinsam mit der Herforder Bitcoin Deutschland GmbH bietet er seinen Kun-

Wer digitalen Speichern nicht traut, kann Bitcoins auch als Papiergeld in den Safe legen.

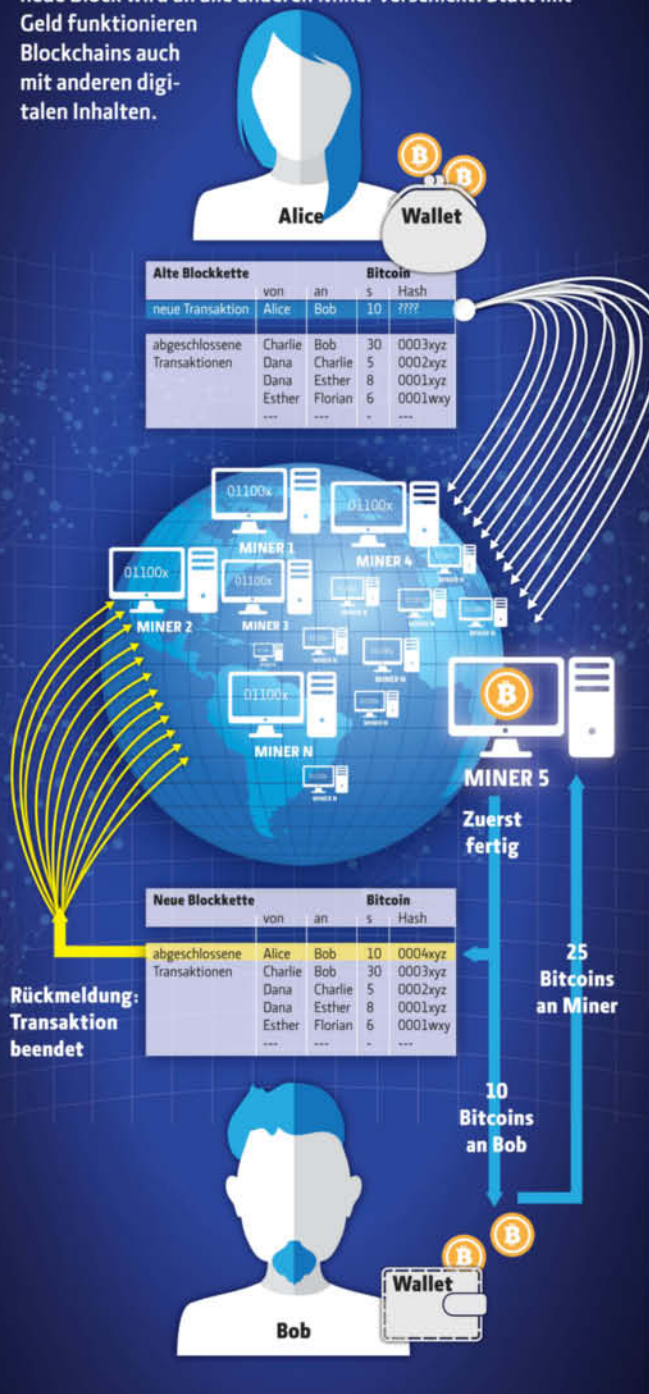


Foto: Ulf J. Froitzheim



Bitcoin: So funktioniert's

Wenn Alice an Bob Bitcoins überweisen will, wird die neue Transaktion – gemeinsam mit Tausenden anderen – an eine Liste verifizierter Überweisungen („Blocks“) angehängt und an alle Miner verschickt. Diese berechnen einen neuen „Hash“, der alle bisherigen Transaktionen zu einem einzigen Wert zusammenfasst. Will jemand Geld ausgeben, das er gar nicht hat, müsste er sämtliche im Umlauf befindlichen Kopien der Blockchain fälschen. Der Miner, der als Erster mit der Berechnung fertig ist, erhält zur Belohnung 25 Bitcoins. Der neue Block wird an alle anderen Miner verschickt. Statt mit Geld funktionieren Blockchains auch mit anderen digitalen Inhalten.



Grafik: Andreas Zickert, www.shutterstock.de

den den An- und Verkauf der Kryptowährung an. Gleichzeitig ist Fidor deutscher Pilotkunde des Blockchain-Spezialisten Ripple Labs.

Ohne Bank, aber mit 300 000 Euro Wagniskapital will das Start-up Pey „normalen“ Menschen das Bezahlen per Bitcoin schmackhaft machen. Der Gründer Ricardo Ferrer Rivero stammt aus Venezuela, hat lange in den USA gelebt und schon mehrere Firmen aus der Taufe gehoben. Er trägt Schulterholster wie die Cops in US-Krimis. Unter der linken Achsel steckt sein Smartphone, rechts sein ungeliebtes Portemonnaie. „Bargeld hat mich immer schon genervt“, sagt Rivero. Also will er es abschaffen. Bisherige Versuche scheiterten an den vielen kleinen Händlern, die nicht einmal Kreditkarten nehmen. Weil bis zu acht Intermediäre an jeder Zahlung mitverdienen, lohnen sich die Gebühren plus Miete fürs Terminal nicht.

Hauptquartier von Pey ist der „Edelstall“, ein loftiger Coworking-Space in Hannovers Szene-Stadtteil Linden. Per 3D-Drucker haben die vier Gründer ein Kassenterminal gebaut – eine kleine Docking-Station für Nexus-Handys. Tippt der Händler den Betrag ein, erscheint ein QR-Code. Der Kunde scannt ihn mit der Pey-App und bestätigt die Zahlung. Dann stellt die App automatisch die Verbindung zur Tauschbörse Bitpay her, die dem Händler sofort den Gegenwert in Euro aufs Bankkonto überweist. Das Ganze funktioniert auch mit Bluetooth und NFC statt mit QR-Code.

Um die Sache ins Rollen zu bringen, beackern die Gründer die Läden und Kneipen der unmittelbaren Nachbarschaft – mit persönlichen Gesprächen, Bitcoin-Verschenkaktionen, T-Shirts, Plakaten, Social-Media-Kampagnen. Doch den größten Anschub versprechen sich die Gründer davon, Arbeitnehmer dazu zu bringen, sich einen Teil des Lohns in Bitcoins auszahlen zu lassen. Bis zu 44 Euro ist das nämlich steuerfrei.

Die Händler müssen für den Dienst noch nichts bezahlen. Erst wenn sich die Transaktionen häufen, möchte Pey mitverdienen. Bitcoin ist dabei nur Mittel zum Zweck. „Die Bitcoin-Community versucht sich von Banken freizuhalten“, sagt Rivero, sieht aber ein: „Nur auf Krypto-Währungen zu setzen ist utopisch.“ Rund 50 Geschäfte und Dienstleister sind derzeit Teil des Lindener „Bitcoin-Boulevards“.

Sollten Bitcoins tatsächlich als alltägliches Zahlungsmittel durchstarten, warten die nächsten Probleme: Die Geldmenge ist auf 21 Millionen Bitcoins begrenzt. Davon sind bereits

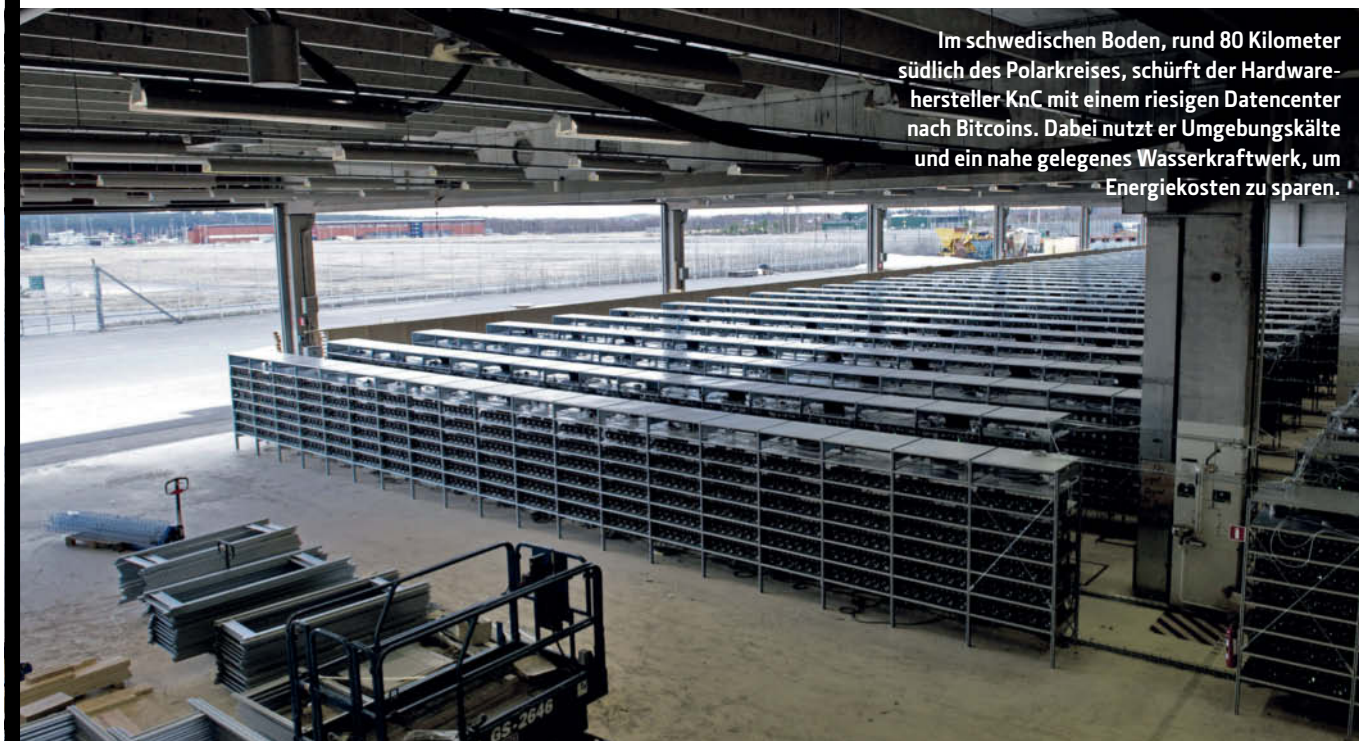
Bitcoin vor der Spaltung

Gerade einmal sieben Transaktionen pro Sekunde schafft das Bitcoin-System – und wird schon aus diesem Grund nie ein globales Zahlensystem werden können. Der Durchsatz ließe sich durch größere Blöcke oder kürzere Takte erhöhen. Die Frage ist nur, wer an den Stellschrauben drehen darf. Erfinder Satoshi Nakamoto selbst tauchte 2011 unter, als der Bitcoin-Hype immer mehr Trittbrettfahrer und Goldgräbertypen anlockte, und hinterließ ein Machtvakuum. Als offiziellen Sachverwalter („Maintainer“) berief er seinen Vertrauten Gavin Andresen, doch der war in dieser Rolle nur der Primus inter Pares. Eine Weile war er „Chefwissenschaftler“ der libertären „Bitcoin Foundation“, in deren Führungsriege sich

immer wieder windige Geschäftsleute drängten. Zwei Funktionäre landeten hinter Gittern: Charlie Shrem wegen Geldwäsche, Mark Karpeles wegen Veruntreuung im Zusammenhang mit dem Bankrott seiner Bitcoin-Tauschbörse Mt. Gox. Dort verschwanden Coins im Wert von Hunderten Millionen Dollar.

Im Sommer lancierte Andresen gemeinsam mit dem Ex-Google-Mann Mike Hearn seine Turbo-Version „Bitcoin XT“ – und provozierte damit bisherige Mitstreiter zu einem offenen Brief, in dem sie sich als die wahren Erben Satoshis darstellten. Neutral sind sie nicht: Allein fünf von ihnen stehen in den Diensten des Bitcoin-Start-ups Blockstream. Firmenchef

Adam Back wirft Hearn vor, mit dem XT-Alleingang den Kollaps des Systems zu riskieren und drei Milliarden Dollar aufs Spiel zu setzen. Aber natürlich dürfte er auch die Zukunft seines Unternehmens im Blick haben. Wie es weitergeht, entscheiden am Ende allerdings weder die Software-Entwickler noch die Eigentümer der 14 Millionen Coins, sondern die Betreiber der Rechnerfarmen und -pools – eine sehr intransparente Szene. Sie hantieren mit großen Beträgen, und jede Änderung des Codes kann für sie horrende Einbußen bis hin zum Totalverlust bedeuten. Wer am Bitcoin-System dreht, muss deshalb mit Verdächtigungen leben. Misstrauen ist die Kehrseite der Trustlessness.



Im schwedischen Boden, rund 80 Kilometer südlich des Polarkreises, schürft der Hardwarehersteller KnC mit einem riesigen Datacenter nach Bitcoins. Dabei nutzt er Umgebungskälte und ein nahe gelegenes Wasserkraftwerk, um Energiekosten zu sparen.

Foto: KnCMiner

14 Millionen im Umlauf. Und das System schafft nur sieben Transaktionen pro Sekunde, denn es produziert nur alle zehn Minuten einen 1-Megabyte-Block. Zum Vergleich: Kreditkartensysteme bewältigen eine fünfstellige Zahl an Buchungen pro Sekunde.

Hinzu kommen die Transaktionskosten. Das Bitcoin-Rechnernetz verbraucht so viel Strom, dass derzeit auf jede Transaktion mehr als fünf Euro an versteckten Kosten entfallen. Laut blockchain.info sind Werte über zehn Dollar keine Seltenheit.

Der Grund für diese Ineffizienz liegt just in jedem Grundgedanken, der Bitcoin für viele so attraktiv gemacht hat: in der „vertrauenslosen“ Sicherheitsarchitektur, die keinen Verant-

wortlichen kennt. An deren Stelle stehen aufwendige kryptografische Berechnungen. Und um die Geldmenge nicht zu schnell ansteigen zu lassen, wird jede Transaktion noch mit einer Rechenaufgabe („Proof of work“) garniert, deren Schwierigkeitsgrad laufend mit der zur Verfügung stehenden Rechenleistung steigt. Das sollte ursprünglich dazu dienen, niemanden zu mächtig werden zu lassen. Doch Privatleute sind bei diesem Rüstungswettlauf längst aus dem Spiel. Knapp drei Viertel der Bitcoin-Produktion stammen heute von fünf großen „Mining-Pools“. Vier von ihnen befinden sich in China, oft in entlegenen Gegenden, wo es kühl und der Strom günstig ist.



Vitalik Buterin ist die treibende Kraft hinter dem Start-up Ethereum.

gäbe hochspannende Möglichkeiten, wenn der Staat seine Grundbücher auf Blockchain-Basis digitalisieren würde“, sagt Oliver Flaskämper, Chef der Tauschbörse bitcoin.de. Ein Hausbesitzer könne dann seine Immobilie unkompliziert in Anteilscheine splitten und für diese separat bei Banken Hypotheken aufnehmen. Notare würden dann arbeitslos: Schließlich ist eine Blockkette nichts anderes als das maschinenlesbare Gegenstück zu einer Notarrolle oder der Journalrolle einer Registrierkasse. Allerdings kann sie nicht nur Bagatellbeträge abwickeln, sondern auch „smart contracts“, also digitale Verträge, die ihre Einhaltung automatisch überwachen – beispielsweise den pünktlichen Eingang von Ratenzahlungen oder Dividenden.

„Wenn man diese Vorgehensweise in andere Bereiche übernimmt, beispielsweise in die Musik oder Fotografie, entstehen digitale Assets, wo

Diesen Sommer begann der Versuch, das Kryptogeld aus diesen Fallen zu befreien. Gavin Andresen, Bitcoiner der ersten Stunde, hob Bitcoin XT aus der Taufe. Aber das Projekt droht am Streit in der Gemeinde zu scheitern (siehe Kasten S. 29).

Die Finanzriesen braucht so etwas nur bedingt zu kümmern. Für die Banken ist die Original-Bitcoin-Kette vor allem ein Proof-of-Concept – mit einer herrlich ironischen Pointe: So stehen Talente aus der kommerzkritischen Open-Source-Subkultur, die gestern noch die Banken abschaffen wollten, heute unverhofft am Scheideweg zwischen Punk und Profit, zwischen Prinzip und Pragmatismus. Der Jobmarkt jedenfalls brummt. Oliver Bussmann, Chief Information Officer der Schweizer Großbank UBS, sprach gegenüber Bloomberg-Reportern von mehr als 100 Firmen, die an der Weiterentwicklung des Blockchain-Konzepts arbeiteten.

Die Ideen betreffen mittlerweile nicht mehr nur den Kapitalverkehr, sondern alle Fälle, in denen Rechte oder Ansprüche dauerhaft dokumentiert oder auf einen neuen Inhaber übertragen werden müssen. Ein Start-up in Kalifornien namens Skuchain konzentriert sich zum Beispiel auf die Dokumentation von Lieferketten. Mögliches Einsatzgebiet ist die Rückverfolgung von Bio-Lebensmitteln vom Verbraucher zum Erzeuger.

Selbst die Arbeit von Behörden könnte sich ändern. „Es

es vorher keinerlei Wertschöpfung gab“, sagt Fidor-Chef Kröner. So ließe sich beispielsweise beim Erwerb eines urheberrechtlich geschützten Songs der Kauf protokollieren – als Nachweis, dass er keine Raubkopie ist. Welche Ideen es bis zur praktischen Umsetzung schaffen, ist noch nicht abzusehen (siehe Übersicht S. 32).

Nur eines scheint ausgemacht: Die Bitcoin-Technologie mag als Kapitalismuskritik begonnen haben – ihr gesellschaftsveränderndes Potenzial entfaltet sie nun Seit an Seit mit dem alten Feindbild. Viele Projekte stehen mit einem Bein noch in der Bitcoin-Welt, mit dem anderen im realen Geschäftsleben. Der Weg zu ihnen ist oft eine veritable Schnitzeljagd. Telefonnummern sind auf den Websites eine Rarität, Anfahrtsskizzen unüblich. Adressen führen oft nur zu Großkanzleien, Treuhändern, Notaren, Holdings oder Büroservices in der Schweiz. In deren Foyers hängen Reihen von Briefkästen. Mancher trägt fünf Firmennamen.

Ethereum, eines der meistbeachteten und ehrgeizigsten Start-ups, residiert am Stadtrand von Baar, im Steuersparparadies und Briefkastenfirmen-Kanton Zug. Die Büros liegen in einem extravaganteren neokubistischen Wohnquader mit Dachterrasse. Entgegen der branchenüblichen Geheimniskrämerei stehen sogar zwölf Klarnamen auf dem Briefkasten. Gavin Wood, einer

der Hauptentwickler, kommt sichtlich überarbeitet die Treppe herunter und öffnet die Glastür, bittet den Besucher aber nicht herein. Zeit für ein Gespräch habe leider niemand aus dem Team – die Deadline für ein Software-Release drückt.

Die junge Mannschaft – zur Zahl der Mitarbeiter äußert sich Ethereum nicht – hat sich vorgenommen, ein komplettes Ökosystem aufzusetzen. Es reicht von einer Blockkette mit eigener Münze, dem „Ether“, über eine Entwicklungsplattform bis zum Browser „Mist“, einer Art Firefox für ein zukünftiges Internet des Geldes. Das Konzept sieht vor, dass jedermann auf Basis dieser Infrastruktur seine eigenen Anwendungen erstellen kann, die sogenannten DApps (Decentralized Applications).

Treibende Kraft des Projekts ist das Mathegenie Vitalik Buterin, ein 21-jähriger Kanadier russischer Abstammung und Schützling des brachiallibertären deutsch-amerikanischen Unternehmers Peter Thiel. Schon als Teenager gab Buterin, ein milchbubig-altkluger Nerd vom Schlag des jungen Bill Gates, das „Bitcoin Magazine“ heraus. Dann wechselte er von der Beobachter- auf die Macherseite.

Die nötigen Ressourcen beschafften sich Buterin und seine lebenserfahrenen Mitstreiter über einen sogenannten Bitcoin-Crowdsale, eine Mischung aus Mikro-Risikokapital und Crowdfunding. Die Förderer überwiesen im Sommer 2014 Bitcoins im Wert von mehr als 15 Millionen Dollar und erhielten dafür Einheiten der Hauswährung Ether, die bei einem Misserfolg verloren wären. Träger des Projekts ist eine Stiftung in der Schweiz. Nähere Fragen zur Konstruktion aus Stiftung und Firma, zum Spagat zwischen Kommerz und Gemeinnützigkeit, beantwortet die Firma nach einigem Hin und Her nicht.

In Baar residiert auch die Bitcoin Suisse AG. Im Obergeschoss eines unpräzisen Gewerbebaus arbeitet CEO Niels Niklas Nikolajsen. Der dunkelhaarige Däne sieht mit Knebelbart und Pferdeschwanz aus wie ein Musketier-Darsteller. Er kam in die Schweiz, weil es dort weniger Regularien für Unternehmer gibt als in der EU. Er hat neben seiner Firma ein zweites Standbein als IT-Dienstleister. Zudem ist er Schweizer Repräsentant der Freien Republik von Liberland. Das ist ein unbewohntes Stück Niemandsland an der Donau, das weder Serbien noch Kroatien haben wollte.

Bei Nikolajsen kann man Bitcoins sogar in Papierform kaufen; wenn man das Geld braucht, rubbelt man den privaten Schlüssel frei und gibt ihn in die Bitcoin-Wallet ein. Damit will er ein analog-digitales Äquivalent zu anonymen Nummernkonten schaffen. Außerdem betreibt er noch eine Handelsplattform und verkauft Bitcoin-Geldautomaten. Obwohl 150-prozentiger Enthusiast, ist er Realist genug, um über das Mining zu lästern: „Wenn ich eine Maschine baue, mit der ich Geld verdienen kann, verkaufe ich sie doch nicht.“

Nicolajsen ist gut vernetzt und hat die Telefonnummer von Johann Gevers im Handy, dem Gründer und Chef der Monetas AG. Der charmante, hagere Hüne mit rotblonder Kurzhaarfrisur nimmt sich spontan Zeit für ein Treffen in seinem schicken neuen Büro in der Baarer Stadtmitte. Seine Monetas AG spart auf ihrer Website nicht mit großen Versprechungen. Sie betreibe die „fortschrittlichste Transaktionsplattform der Welt“, löse „eine der größten Herausforderungen der Menschheit“ und biete allen Beteiligten „unglaublichen Nutzen“. Gemeint ist damit ein Blockchain-basiertes Zahlungssystem, mit

dem beispielsweise Arbeitsmigranten aus armen Ländern zu geringstmöglichen Kosten Geld an ihre Familien überweisen können.

Im persönlichen Gespräch wird klar: Das angeberische Marketingbohei auf monetas.net passt gar nicht zum Naturell von Johann Gevers. Der 50-Jährige ist Spross einer norddeutschen Missionarsfamilie, die im 19. Jahrhundert nach Südafrika ausgewandert war. Er ist ein sanfter, offener Typ, der glaubt, was er sagt. Von Haus aus Kaufmann, hatte er schon als Wirtschaftsprüfer, Vermögensverwalter und Unternehmensberater gearbeitet, bevor er mit Patri Friedman zusammenkam. Der Enkel des berühmten Ökonomen Milton Friedman ist Gründer der libertären „Seasteading“-Bewegung, die

Ricardo Ferrer Rivero will Bitcoins als Zahlungsmittel für Normalverbraucher etablieren. Für Werbekampagnen schleppt er mit seinen Mitstreitern schon mal einen 60 Kilogramm schweren Geldautomaten (im Hintergrund) in der Nachbarschaft herum.



Foto: Simon Kondermann



auf schwimmenden künstlichen Inseln herrschaftsfreie Kommunen gründen wollte. 2011 engagierte er den Wahlkanadier Gevers als Projektmanager für eine „Freie Stadt“ in Honduras, ein privat finanziertes soziales Experiment auf dem Festland, das sich aus politischen Gründen dann doch nicht realisieren ließ.

Es war die Zeit, als Bitcoin bekannt wurde und rasch Amerikas Libertarians verzückte. Auch Gevers, der sich schon früher für digitales Geld interessiert hatte, wurde neugierig. Gemeinsam mit einem amerikanischen Softwareentwickler konzipierte er die auf Bitcoin aufsetzende Monetas-Software. Der Prototyp funktionierte, doch der Kaufmann in Gevers wusste, dass das Ergebnis weit weg war von einem Produkt, das er seiner Zielgruppe hätte verkaufen können: Banken, die mit neuen Dienstleistungen neue Kunden ansprechen wollen. Eigentlich sieht der Monetas-Gründer – ganz im Einklang mit der Bitcoin-Szene – Geldinstitute umso kritischer, je größer sie sind. „Das Finanzsystem ist zu zentralisiert“, erklärt er in seiner unaufgeregten Art. „In einem dezentralen System ist das so: Wenn der Einzelne einen Fehler macht, hat er Pech. Aber nicht alle anderen.“

Als Pragmatiker und bekennender Anhänger des Kapitalismus sagt er allerdings nicht Nein, wenn er seine Software an Großbanken verkaufen kann, die damit ihrerseits Menschen in armen Ländern erschwinglichere Überweisungsdienste anbieten können. Deshalb engagierte er erfahrene Softwareingenieure, die den Code von Grund auf neu schrieben. Inzwischen hat die Vermarktung begonnen, und Monetas könnte eine der ersten kommerziellen Blockchain-Anwendungen werden.

Das Prinzip basiert auf „Colored Coins“. Das „Färben“ verwandelt Bitcoins oder Bruchteile davon in „Tokens“, also Wertmarken, die Gegenstände oder Ansprüche in der realen Welt repräsentieren – etwa ein Guthaben in irgendeiner anderen Währung oder ein Auto. Das widerspricht zwar der reinen Lehre. Aber während das Risiko bei Bitcoin-Transfers allein beim Endverbraucher liegt, verlagert es sich in dieser Form auf den Betreiber. Dieser muss freilich, wie in der Prä-Bitcoin-Ära, um das Vertrauen seiner Kunden werben. Sollte das Bitcoin-System jedoch kollabieren, hinge auch Monetas in der Luft.

Bei Ripple Labs (siehe TR 5/2014, S. 44) kann so etwas nicht passieren. Das Unternehmen ist der Branchenpionier schlechthin und wird den „Agnostics“ zugerechnet. Sprich: Es hat mit der

Die neue Finanzwelt

Firma	Produkt	Macher und Finanziers
Blockchain	An die Bitcoin-Blockchain werden Nebenketten „angedübelt“, auf denen Geschäftsvorfälle nicht öffentlich abgelegt werden. Bitcoin dient als Sicherheitsinfrastruktur.	Mehrere Mitglieder der Bitcoin-Kernmannschaft. Interessenkonflikte sind möglich. Viele Silicon-Valley-Größen unter den Investoren.
Ripple Labs	Von Bitcoin unabhängiges System, das sich für Finanztransaktionen innerhalb eines Teilnehmerkreises eignet, in dem gegenseitiges Vertrauen herrscht. Statt Coins verwendet es eine haus eigene Wertmarke namens XRP.	Heterogene, interdisziplinäre Mannschaft bis hin zum Ex-NSA-Mitarbeiter. Geldgeber: Andreessen Horowitz, Google Ventures, IDG Capital.
Factom	Kryptografische Fingerabdrücke von digitalisierten Dokumenten (nicht diese selbst) werden in die Bitcoin-Blockchain eingebaut, um bei Bedarf die Echtheit zu überprüfen.	Team von Informatikern und Kaufleuten, Erfahrung mit Immobilien. Neben dem Open-Source-Projekt existiert eine Firma, die Investoren sucht.
Ethereum	Arbeitet mit eigener Blockchain. Die interne „Währung“ ist Mittel zum Zweck, kein Geldersatz. Das Ziel ist es, beliebige Vorgänge kryptografisch abzusichern.	Softwareleute mit Bitcoin-Erfahrung. Das Startkapital kam per Crowdfunding zusammen; wie es weitergeht, ist noch unklar.
Monetas	Senkt die Kosten für internationalen Geldverkehr. Setzt auf die Bitcoin-Blockchain auf, wird aber von Finanzdienstleistern betrieben und funktioniert mit normalen Währungen.	Gründer mit kaufmännischem Background, unterstützt von privaten Investoren.
Hyperledger	Konkurrenz zu Ripple, verzichtet aber auf Coins samt dem Aufwand für ihre Erzeugung. Gedacht für schnelle Finanztransaktionen zwischen Banken. Diese können beliebig viele Blockchains für spezifische Zwecke anlegen.	Wurde vom Finanzspezialisten Digital Assets aufgekauft. Führende Mitarbeiter haben Banking-Erfahrung.
Clearmatics	Geplante Clearing-Plattform für außerbörslichen Handel; nutzt die Ethereum-Blockchain und erlaubt programmierbare Geldanlage-Produkte („smart contracts“).	Gründer Robert Sams kommt aus dem Derivate-Handel, sein Partner ist der Genfer Software-Unternehmer Alexandre Callea.
Coinbase	Erste Bitcoin-Börse, die von mehreren US-Bundesstaaten lizenziert wurde. Hilft Konzernen, Bitcoin-Zahlungen ohne Währungsrisiko entgegenzunehmen.	Zu den Investoren zählen Banken und die New Yorker Börse.

Ideologie der Bitcoin-Szene nichts am Hut. Die 100 Mitarbeiter sitzen im Finanzdistrikt von San Francisco und haben sich darauf spezialisiert, die IT der bestehenden Banken mithilfe der Blockchain-Technologie auf Trab zu bringen. Es gibt kein langsames, energieverschwendendes Proof-of-work, denn die Netzknoten werden von bekannten Partnern betrieben, die einander trauen. Deshalb benötigt es auch kein Münzen-Mining. Die „XRP“ genannten Coins dienen lediglich dazu, pro Transaktion eine kleine Bearbeitungsgebühr zu erheben. Im Devisengeschäft ersetzen sie den Dollar als Brückenwährung zwischen „illiquiden“ Währungspaaren, die wegen eines zu geringen Handelsvolumens nicht zu einem fairen Kurs direkt umgetauscht werden können.

Ripples deutscher Referenzkunde ist die Fidor Bank. Auf die Frage, ob die Zusammenarbeit für ihn schon mehr sei als ein Experiment, antwortet Vorstandschef Matthias Kröner in einer E-Mail ausweichend: „Ripple hilft Banken, Auslandsüberweisungen in Echtzeit zu günstigen Kosten anzubieten. Wir halten Ripple für eine spannende Innovation, die sich jede Bank ansehen sollte.“ Seine Kollegen in den großen Häusern sehen das offenbar ähnlich. ABN Amro, Citibank, Deutsche Bank und UBS wagen sich zwar noch nicht an Pilotprojekte, aber ihre Informatiker und Juristen verfolgen die Blockchain-Szene genau.

Eine der entscheidenden Fragen ist eher rechtlicher als technischer Natur: Wenn der Münzbesitzer seinen privaten Schlüssel (ein sehr langes Passwort) verliert oder ihm das Handy mit Wallet-App gestohlen wird, ist das Geld ohne ein Backup unwiederbringlich weg. Das darf bei einer Blockchain, an der die Eigentumsrechte an Häusern, Autos, Aktien oder Kunstwerken hängen, nicht passieren. Und eine Blockchain, die nur eine Kopie des Grundbuchs, Kfz-Registers oder Echtheitszertifikats wäre, bringt wenig Nutzen. An einem Ausweg aus diesem Grunddilemma arbeiten nach eigenem Bekunden viele Start-ups. Eine Lösung ist allerdings noch nicht auf dem Markt.

Worin allerdings tatsächlicher Nutzen bestehen könnte, verriet sein Kollege Matthijs Geneste von der ABN Amro Clearing Bank: Vielleicht könnten Banken eines Tages normale Währungen wie den Euro an die Blockkette legen – natürlich unter den Fittichen der jeweiligen Zentralbank. Das könnte beispielsweise den internationalen Geldtransfer vereinfachen und günstiger machen. Wenn es so weit kommen sollte, hätte Satoshi Nakamoto mit seiner Technik das etablierte Bankensystem eher gestärkt denn überflüssig gemacht – das glatte Gegenteil von dem, was er erreichen wollte.



MESSE
NETWORKING
KONGRESS
FACHFOREN

EUROPAS FÜHRENDE ENERGIEFACHMESSE

E-WORLD ENERGY & WATER

16. - 18.2.2016
ESSEN, GERMANY

24.000
FACHBESUCHER

BESUCHER AUS 80 NATIONEN

640
AUSSTELLER

AUSSTELLER AUS 25 NATIONEN

www.e-world-essen.com

MESSE
ESSEN

con energy

Plasma statt Antibiotika

Geräte, die mit ionisierten Edelgasen Keime abtöten, halten gerade Einzug in die Arztpraxen. Sie heilen nicht nur chronische Wunden, sondern können sogar **Gewebe regenerieren und Krebszellen abtöten.**

VON UTA DEFFKE

Ein Fiepen liegt in der Luft. Carsten Gutgesell fährt mit einem dicken Stift über eine Wunde am Bein des Patienten Hannes Vogel (Name von der Redaktion geändert), als wolle er sie ausmalen. Doch statt einer Mine kommt aus der fiependen Spitze eine zentimetergroße, feine Flamme. In ihr liegt das Geheimnis dieser Behandlungsmethode: Die Flamme ist nicht heiß – sondern kalt. Es handelt sich um sogenanntes kaltes Plasma. Auf der Haut spürt Vogel davon nur ein feines Prickeln und einen Luftzug aus der Düse. „Es tut gar nicht weh“, sagt er.

Gutgesell behandelt in seiner Norderstedter Praxis häufig schlecht heilende Hauterkrankungen wie die von Hannes Vogel. Bei älteren Diabetes-Patienten sind es oft chronische Wunden, die zum Beispiel durch Keime mitverursacht werden können und oft über Wochen, Monate oder gar Jahre nicht heilen. Das ist nicht nur schmerzhaft, sondern birgt die Gefahr einer Infektion und möglicherweise sogar einer Blutvergiftung (Sepsis).

Typische Fälle seien aber auch „das offene Bein, Pilzkrankungen der Haut und des Nagels sowie Warzen, die durch Viren, und Akne, die durch Akne-Bakterien hervorgerufen werden“, erklärt der Hautarzt. Wo Wundreinigung, antibakterielle Verbände, Antibiotika oder Anti-Pilz-Mittel nicht mehr helfen, beobachtet Gutgesell oft schon nach wenigen Behandlungen mit dem kalten Plasma einen Heilungsfortschritt. So auch bei Hannes Vogel: Seine Wunde beginnt sich endlich zu schließen.

Kalte Plasmen sind derzeit ein heißes Thema in der Medizin. Weil sie Mikroben zuverlässig abtöten – vor allem auch multi-resistente Keime, ohne selbst Resistenzen zu erzeugen –, kamen sie zuerst in der Wundheilung zum Einsatz. Die Erfolge sind mittlerweile in zahlreichen klinischen Studien belegt. Die ersten Geräte wurden bereits als Medizinprodukte zugelassen und

halten gerade Einzug in die Arztpraxen. In Laborexperimenten mit Hautzellen zeigte sich sogar noch eine weitere überraschende Eigenschaft: Unter Einfluss der Plasmen bildet sich auch neues Gewebe.

Damit bietet kaltes Plasma einen wesentlichen Vorteil gegenüber herkömmlichen Mitteln. Denn die töten Bakterien und Pilze zwar ab, können jedoch das Heilen behindern, erklärt Thomas von Woedtke. Der Pharmazeut hat seit 2011 die weltweit erste Professur für Plasmamedizin inne. Er lehrt und forscht an der Universität Greifswald und am Leibniz-Institut für Plasmaforschung und Technologie (INP). Hier ist das deutschlandweit größte Zentrum für Plasmamedizin. Weitere gibt es etwa in Bochum, München und Göttingen.

Plasmen sind bisher eher aus der Physik und Technik bekannt. Es handelt sich um Gase, deren Moleküle durch Energiezufuhr, zum Beispiel als Strom oder Wärme, in negativ geladene Elektronen und positiv geladene Ionen aufgespalten werden. So sind etwa Blitze und die Sonne viele Millionen Grad heiße Plasmen. In Kernfusionsreaktoren sollen sie künftig, von starken Magneten gebündelt, Energie liefern. Und in Plasma-bildschirmen regen sie – hier weniger heiß – Leuchtstoffe zur Lichtabgabe an. In der Medizin werden heiße Plasmen bereits seit den 1960er-Jahren eingesetzt, vorwiegend um Instrumente zu sterilisieren, aber auch um Blutgefäße zu veröden. Doch erst seit den Neunzigerjahren ist es möglich, auch kalte Plasmen zu erzeugen, die körperverschträgliche Temperaturen unterhalb von 40 Grad Celsius haben.

Als Ausgangsstoff dienen oft die Gase Argon oder Helium. Unter Energiezufuhr bewirken sie in der Umgebungsluft die Entstehung hochreaktiver Stickstoff- oder Sauerstoff-Radikale sowie UV-Strahlung. „Dies ist entscheidend für das Abtöten von Mikroorganismen“, erklärt von Woedtke. Zusätzlich reißt das

Foto: TU Eindhoven

elektromagnetische Feld des Plasmas vorübergehend Löcher in die Membran der Bakterien- und menschlichen Zellen. Durch sie gelangen die reaktiven Substanzen ins Innere. Weil das Erbgut von Bakterien nicht durch einen Zellkern geschützt ist, so die Vermutung der Forscher, reagieren sie empfindlicher als menschliche und tierische Zellen auf die Erstürmung. Bei letzteren entstehen durch die kurze Einwirkzeit des Plasmas nach jetzigem Wissensstand keine Schäden. Die elektromagnetischen Felder können die Bakterien aber auch direkt abtöten.

Wie die kalten Plasmen die Geweberegeneration bei den Patienten bewirken, ist weniger klar. Sie scheinen zum Beispiel Gene zu aktivieren, die in den Zellen Reparaturmechanismen in Gang setzen sowie Zellwachstum und Zellteilung anregen.

Könnten sie dann nicht auch ein unkontrolliertes Zellwachstum befördern und Krebs verursachen? Bislang sind keine bedenklichen Folgen beobachtet worden, wie deutsche Forscher vom Nationalen Zentrum für Plasmamedizin 2014 in einem Positionspapier schrieben. „Wir wünschen uns trotzdem große Studien zur weiteren Untersuchung der Sicherheit“, sagt von Woedtke.

Dennoch gilt eher im Gegenteil kaltes Plasma als mögliche neue Waffe für die Tumorbildung. Einer der Pioniere ist Hans-Robert Metelmann, Direktor der Klinik und Poliklinik für Mund-Kiefer-Gesichtschirurgie in Greifswald. Er behandelt meist Patienten mit Krebserkrankungen im Kopf-Hals-Bereich im fortgeschrittenen Stadium. „Mit dem Plasma können wir die Belastungen für die Patienten reduzieren, die mit einem Bakterienbefall der [zum Teil offen liegenden] Tumoren einhergehen: die Sepsis-Gefahr, den Geruch und den Einsatz von Schmerzmitteln mit deren erheblichen Nebenwirkungen“, sagt Metelmann.

Da die Plasmabehandlung nur an der Oberfläche wirkt, „werden wir damit keine Massentfernung von Tumoren machen“, sagt der Mediziner. Sie ließe sich aber nach dem Herausschneiden der Geschwulst als Alternative zu den aggressiven Bestrahlungs- oder Lasermethoden einsetzen: Zum Beispiel um an schlecht erreichbaren Stellen wie im Kiefer oder an kritischen Stellen wie der Schlagader liegende Tumorreste zu beseitigen. Potenziell ließen sich damit auch übrig gebliebene, aber nicht erkennbare Krebszellen ausmerzen. Denn das Plasma setzt offenbar die sogenannte

Apoptose wieder in Gang, eine Art Selbstzerstörungsprogramm für kranke Zellen, das Krebszellen meist ausgehebelt haben. Danach dauert es nur ein bis zwei Tage, bis sich gesunde Ersatzzellen bilden. So entsteht kein Loch im Gewebe.

Für engräumige Behandlungen wie bei verwinkelten kleinen Tumoren oder Zahnwurzelbehandlungen arbeiten Techniker am INP bereits an Prototypen von flexiblen Plasma-geräten mit feineren Plasmajets. „In die Anwendung und medizintechnische Zulassung müssen das dann Unternehmen bringen“, sagt von Woedtke. Aber auch hier ist das INP mit von der Partie: neoplas tools etwa ist ein Spin-off, das den von Gutgesell genutzten Plasma-Pen entwickelt hat.

Ein weiteres, bereits mit Förderpreisen bedachtes INP-Spin-off ist Coldplasmatech. Weil die händische Behandlungsweise, wie sie etwa Carsten Gutgesell praktiziert, zeitaufwendig und deshalb kaum wirtschaftlich ist, hat sich Coldplasmatech eine neue Technik ausgedacht: Eine etwa schokoladentafelgroße, flexible Wundauflage auf Silikonbasis. Sie wird so über die Wunde gelegt, dass darüber ein abgeschlossener Hohlraum entsteht. Darin wird per Hochspannung ein Plasma gezündet, das einige Minuten gleichmäßig auf die gesamte Fläche einwirkt, ohne dass der Arzt später ständig dabeisitzen muss. Noch ist weitere Entwicklungsarbeit nötig. Doch Mitgründer und Medizinökonom Tobias Güra hofft, den Zulassungsantrag als Medizintechnikprodukt bis Jahresende einreichen zu können.

Der „kINPen MED“ von neoplas tools ist das erste in Deutschland zugelassene Kaltplasma-Behandlungsgerät für Wunden.



Foto: neoplas tools



Tausendfüßler im Eis

Die britische Halley VI ist die mit Sicherheit ungewöhnlichste Forschungsstation in der Antarktis. **Die Gebäude stehen auf Skiern, damit sie alle paar Jahre den Ort wechseln können.** Der Entwurf stammt vom Architekten Hugh Broughton, und nicht von ungefähr erinnert das Design an eine futuristische TV-Serie aus den 60er-Jahren.

INTERVIEW: ROBERT THIELICKE



Halley VI steht auf dem Brunt Ice Shelf der Antarktis. Die Beine enden in Kufen, damit die Forschungsstation an andere Orte gezogen werden kann. Sie sind zudem hydraulisch höhenverstellbar, um die Module schrittweise anzuheben. Sonst würden sie langsam im Schnee versinken, denn um Halley herum bleiben pro Jahr 1,5 Meter Schnee liegen.

TECHNOLOGY REVIEW: Bevor Sie die britische Forschungsstation in der Antarktis planten, war Ihr größtes Projekt die Hauptverwaltung der Pfadfinderinnen in Wimbledon. Sie waren nicht der perfekte Kandidat für Halley VI, oder?

HUGH BROUGHTON: Stimmt, ich hatte überhaupt keine Erfahrung mit dieser Art von Projekt. Der Bau für die Pfadfinderinnen war gerade einmal 200 Quadratmeter groß und kostete etwa 200 000 Euro. Für den Architektur-Wettbewerb zu Halley VI aber setzte das British Antarctic Survey folgende Kriterien fest: Es sollte ein großes, multinationales Büro sein und viel Erfahrung damit besitzen, vorfabrizierte Module für Forschungszwecke zu errichten. Und das alles unter extremen Umweltbedingungen und möglichst nachhaltig. Nichts davon konnten wir vorweisen. Wir starteten nicht unbedingt von der Poleposition.

Sie waren vorher noch nicht einmal in der Antarktis. Nein, es ist ja auch nahezu unmöglich, dorthin zu gelangen.

Warum fiel die Wahl trotzdem auf Sie?

Ich ging zur Auftaktveranstaltung des Wettbewerbs im Juli 2004. Dort traf ich einen Ingenieur einer Firma namens AECOM, mit der ich schon zusammengearbeitet hatte. Er sagte: Lass uns das gemeinsam versuchen. AECOM fand dann unter ihren Angestellten Ingenieure, die seit Jahren für das amerikanische Antarktis-Programm arbeiteten. Sie halfen uns über die Ziellinie.

Woher wussten Sie, was Menschen in diesem Landstrich benötigen?

Zum einen stellte der British Antarctic Survey sehr umfangreiches Material zur Verfügung. Außerdem besprachen wir uns viel mit Leuten, die einige Zeit in der Antarktis verbracht haben. Wir wollten wissen: Was sind die sozialen und psychologischen Herausforderungen? Wir überlegten uns, was die Bewohner vom Aufstehen bis zum Zubettgehen alles taten und wie das dazu passende Design aussehen musste. Wenn sie aufstehen, soll da ein Teppich sein? Oder ein Holzfußboden? Muss man vor dem Badezimmer anstehen, oder soll jeder sein eigenes haben?

Sie entwarfen also ein Wohnzimmer für den extremsten Ort der Welt. Gaukelt das nicht eine Sicherheit vor, die dort nicht existiert?

Das ist tatsächlich ein wichtiger Punkt. Einige Forscher vergessen in dieser komfortablen Umgebung, dass draußen minus 30 oder minus 40 Grad Celsius herrschen. Wenn etwas schiefgeht, stehen sie plötzlich der Fragilität ihrer Existenz dort gegenüber. Vor ein oder zwei Jahren etwa fielen Strom und Heizung aus, weil die Kühlung für den Generator beschädigt war. Niemand kam zu Schaden, aber die Bewohner sahen sich von einem Moment auf den nächsten einer ziemlich gefährlichen Situation gegenüber. Man vergisst die harte Realität leicht, wenn man beim Abendessen Rotwein trinkt und Roastbeef isst.





Wann waren Sie das erste Mal in der Antarktis?
Anfang Januar 2006.

Wie war es?

Wir flogen zur Position der Station, die wir bauen sollten. Unten war es topfeben, komplett weiß, es gab keine besonderen landschaftlichen Merkmale, kein Leben. Ich dachte: Oh mein Gott, was für ein hoffnungsloser Ort. Aber nach ein oder zwei Tagen bemerkt man die kleinen Unterschiede, die Art, wie der Wind über den Schnee bläst, die verschiedenen Wolkenformationen, das Glitzern der Sonnenstrahlen auf dem Eis. Man wird verführt. Die Leere ist spektakulär.

Kamen Sie dort auf die Idee, die Gebäude auf Skier zu stellen?

Oh nein, das war unsere Idee von Anfang an. Der Untergrund ist kein Fels, sondern Schelfeis, das vom Kontinent ins Meer strömt. Sollte die Eisplatte abbrechen, wäre die Forschungsstation weg. Tatsächlich hatte der British Antarctic Survey bereits vier Stationen auf diese Weise verloren, die fünfte war auf dem besten Weg dahin, und ein sechstes Mal sollte das nicht passieren. Also musste man sie verlagern können. Wir sahen auf Bildern die riesigen Schlitten, die in der Antarktis als Transportvehikel dienen. Also dachten wir: Unser Gebäude muss wie ein gigantischer Schlitten sein.

Funktioniert es?

Wir haben die Module 15 Kilometer von ihrem Bestimmungsort entfernt aufgebaut, um die alte Station als Basis nutzen zu

können. Anschließend haben wir die Module an die neue Stelle gezogen. Das hat geklappt. Der nächste Umzug steht in zwei oder drei Jahren an.

Als Kind waren Sie ein Fan der futuristischen TV-Serie „Thunderbirds“ aus den 60er-Jahren. Ist sie der Grund für das ungewöhnliche Design?

Oh, das ist lustig. Es gibt dieses fantastische Kinderbuch „The Thunderbirds Cross-sections“ mit dreidimensionalen Aufrisszeichnungen. Das war unser ästhetischer Referenzpunkt. Dem, der die Computergrafiken für uns herstellte, zeigten wir es und sagten: So etwa in der Art wollen wir es haben. Früh in der Designphase wollten wir zudem unbedingt Beine, die schräg nach außen standen. Aber der Ingenieur rief uns an und sagte: Es wird euch nicht gefallen, aber wir müssen sie vertikal konstruieren. Ich hielt das für keine gute Idee. Aber er sagte: „Ich habe nachgeschaut, in ‚Thunderbirds Cross-sections‘ besitzt das Flugzeug Thunderbird II auch vertikale Beine.“ Beim Landen fahren sie aus. Wir wären also etwas originalgetreuer. Wir haben sogar die Hydraulik eingebaut.

Warum das?

In dieser Gegend lagern sich jährlich rund 1,5 Meter Schnee ab. Er schmilzt nie, irgendwann würde die Station unter einer weißen Decke verschwinden. Also entwickelten wir hydraulische Beine. Jedes lässt sich einzeln einziehen. Man schaufelt Schnee darunter und setzt es wieder ab. So hebt man Bein um Bein das ganze Gebäude.



Das Kommunikationszentrum kontrolliert unter anderem den Luftverkehr rund um die Station.

Foto: James Morris

Das Zentralmodul ist der Gemeinschaftsraum. Auf 479 Quadratmetern finden sich unter anderem Essraum, Bar, ein Billardtisch – und eine gemütliche Sofaecke.

Foto: James Morris

Am Ende kostete das Projekt 50 Millionen Euro, 250-mal mehr als das Gebäude für die Pfadfinderinnen. Hatten Sie irgendwann einmal gedacht: Das ist eine Nummer zu groß für mich? Nein, absolut nicht. Wir hatten den Wettbewerb gewonnen! Ich sah es als meine große Chance. Natürlich gab es immer wieder große technische Schwierigkeiten, und man verstrickte sich darin. Aber dann haben wir uns gesagt: Moment mal, wir arbeiten in der Antarktis. So wenig Menschen bekommen diese Gelegenheit, also denk dran, wie viel Glück du hast.

Was war denn Ihr größtes Problem?

Um ehrlich zu sein, die Verbindung von Außenhaut und tragendem Stahlgerüst. Beides arbeitet, insbesondere wenn die Station auf Schneehöhe angehoben oder auf Skiern gezogen wird. So etwas hatte noch niemand zuvor gemacht.

Mit Halley VI haben Sie eine Art Architekten-Wettlauf losgetreten. Auch andere Länder wollen nun schicke Stationen in der Antarktis.

Halley VI war tatsächlich eine Art Kick-off, ein erster Schritt hin zu einer neuen antarktischen Architektur. Andere Nationen begannen ebenfalls, Wettbewerbe auszuschreiben. Wir wurden

oft eingeladen mitzumachen. Zwei haben wir gewonnen: für eine spanische Antarktisstation und für eine amerikanische Station auf Grönland.

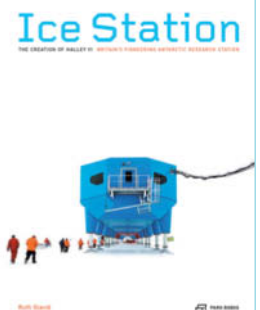
Was ist als Nächstes dran? Vielleicht eine Station auf dem Mars?

Ja, wirklich. Wir arbeiten gerade mit der Nasa im Hinblick auf eine künftige Marsmission zusammen. Die Möglichkeiten, im tatsächlichen Designprozess eine Rolle zu spielen, dürften zwar sehr begrenzt sein. Aber es ist spannend, sich in diesem frühen Stadium Gedanken zu machen.

Menschen, die da waren, können sie diesmal leider nicht fragen.

Das stimmt. Obwohl – am Ende findet AECOM auch dafür einen, den man anrufen kann.

Die Bilder stammen aus dem Buch „Ice Station – The Creation of Halley VI“ (engl.), Ruth Slavid, Park Books, 2015, 29 Euro





Im oberen Stockwerk des Zentralmoduls befinden sich eine Lounge mit Besprechungstisch und sogar ein Fitnessraum.

Foto: James Morris



Die Schlafzimmer wurden komplett vorfabriziert, alle Möbel bereits eingebaut.

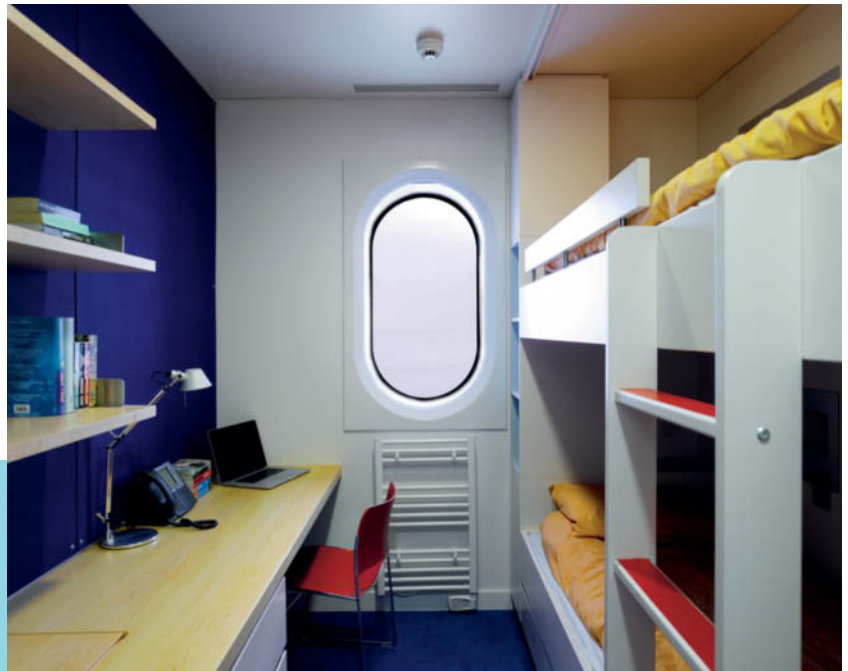


Foto: James Morris



Die Krankenstation erlaubt kleinere Operationen sowie zahnmedizinische Eingriffe.



Die Module stehen vier Meter über dem Eis, die Skier sind 3,90 Meter lang und 1,10 Meter breit. Die blauen Module sind 152 Quadratmeter groß und knapp 20 Meter lang, das rote Zentralmodul mit den Gemeinschaftsräumen misst etwas über 28 Meter.



Wie klug wird Facebook?

Mit künstlicher Intelligenz will das soziale Netzwerk seinen Dienst zum Leben erwecken – und zum **digitalen Assistenten für den Alltag machen.**

Ein Besuch in Facebooks KI-Zentrale.

VON TOM SIMONITE

Pionier der neuronalen Netze: Yann LeCun will Software beibringen, Sprache wie ein Mensch zu verstehen.

Foto: Thomas Ehnemann

Vor zwanzig Jahren hat Yann LeCun schon einmal versucht, die künstliche Intelligenz neu zu erfinden. Beinahe zehn Jahre lang hatte der junge Franzose eine Idee verfolgt, von der viele seiner Informatiker-Kollegen gar nicht viel hielten: dass die Imitation einzelner Gehirnfunktionen der beste Weg sei, intelligente Maschinen zu erschaffen. Bei den Bell Labs entwickelte er eine Software, die Neuronen simulierte, um Handschrift zu lesen. 1995 war LeCun so weit: Bell

Labs' Muttergesellschaft AT&T vermarktete die ersten Maschinen, die handgeschriebene Schecks und Formulare einlesen konnten.

Doch während LeCun gerade die Einführung seiner Bankautomaten feierte, kündigte AT&T die Aufspaltung des Konzerns in drei Einzelunternehmen an. LeCun wurde zwar Forschungsleiter einer verschlankten AT&T, er sollte aber künftig an anderen Projekten arbeiten.

Doch LeCun trieb seine Idee zusammen mit einer Handvoll anderer unbeirrt voran – durch zwei Jahrzehnte voller Gleichgültigkeit und gelegentlich offener Ablehnung aus dem Kollegenkreis. Heute ist sie unter dem Namen Deep Learning bekannt. Google, Microsoft, Baidu und andere wetten, wer diese Technologie, mit der sich eindrucksvolle Erfolge bei der Gesichts- und Spracherkennung erzielen lassen, als Erster in Produkten einsetzt.

Und auch diesmal ist LeCun wieder vorn mit dabei, diesmal im Auftrag von Facebook. Das Unternehmen warb ihn im Dezember 2013 von der New York University ab und ernannte ihn zum Leiter eines neuen Forschungsteams für künstliche Intelligenz (KI). Die Abteilung, Fair genannt (für Facebook AI Research), hat zurzeit 50 Mitarbeiter, soll aber auf 100 wachsen. LeCuns Gruppe ist damit Facebooks erstes ernsthaftes Investment in Grundlagenforschung.

LeCun will Software mit Sprachfähigkeiten und „gesundem Menschenverstand“ entwickeln, die einfache Konversationen beherrscht. Statt mit Maschinen über Mausklicks oder sorgfältig ausgewählte Suchbegriffe zu kommunizieren, würden wir ihnen einfach erzählen, was wir wollen – als sprächen wir mit einer Person. „Unsere Beziehung mit der digitalen Welt wird sich durch intelligente Agenten, mit denen Sie interagieren können, komplett verändern“, verspricht er.

Derartige Kunststücke sind mit heutiger Technik nicht möglich. Apples Siri versucht

Vorbild
Silicon Valley:
Entwickler im
neuen New
Yorker Büro
von Facebook.

zum Beispiel, Sprachbefehle in eine kleine Anzahl von Kategorien einzusortieren, die festgelegte Reaktionen auslösen. Andere Systeme, wie IBMs „Jeopardy!“-Gewinner Watson, meistern zwar scheinbar komplexe Sprachaufgaben, sind jedoch hochspezialisiert auf bestimmte Aufgabengebiete.

Im Gegensatz dazu sollte „tieflernende“ Software in der Lage sein, Sprache ähnlich zu interpretieren, wie Menschen es tun. Den ersten Schritt hat LeCuns Team bereits geschafft: Es hat ein System entwickelt, das eine einfache Geschichte lesen und Verständnisfragen beantworten kann. Es nutzt dabei Fähigkeiten wie logisches Schließen und ein rudimentäres Verständnis von Zeit.

Die Wurzeln dieser Technologie reichen weit zurück: Die Kernidee war von Anfang an, dass sich Verbindungen zwischen Neuronen umso mehr verstärken, je öfter diese Zellen miteinander kommunizieren. 1956 verwendet der Psychologe Frank Rosenblatt diese Theorien zur einfachen Simulation neuronaler Netze in Software und Hardware. Rosenblatts Perzeptron, wie er seinen Entwurf nannte, konnte lernen, einfache Bilder in Kategorien – zum Beispiel Dreiecke und Quadrate – einzusortieren.

Seine Idee wurde zu einem Dreh- und Angelpunkt des damals neu entstehenden Forschungsgebiets künstliche Intelligenz. Schon bald, versprach Rosenblatt, wären Perzeptrons mit mehreren sukzessiven Stufen des Lernens in der Lage, beispielsweise Menschen mit ihrem Namen zu begrüßen.

Doch leider erfüllte Rosenblatts Algorithmus nicht die Erwartungen seines Schöpfers. 1969 veröffentlichte der KI-Pionier Marvin Minsky, der mit Rosenblatt auf die Highschool gegangen war, eine vernichtende Kritik. Minsky wies nach, dass auch Perzeptron-Netzwerke mit mehreren Schichten nicht mächtig genug werden könnten, um von praktischem Nutzen zu sein. Die meisten KI-Forscher gaben die Idee auf.

Nicht jedoch LeCun. Er war fasziniert, als er in den frühen 1980er-Jahren als Ingenieurstudent in Paris von Perzeptrons las. Ganze Tage verbrachte er in einer Forschungsbibliothek nahe

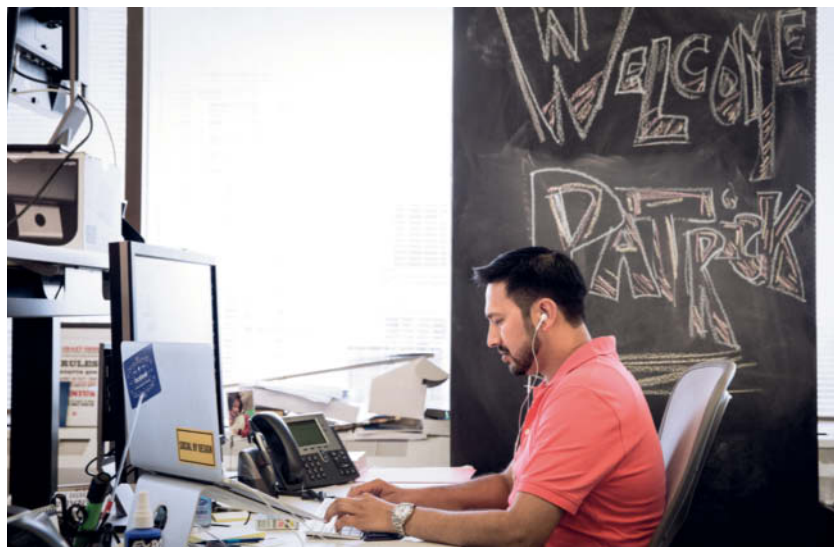
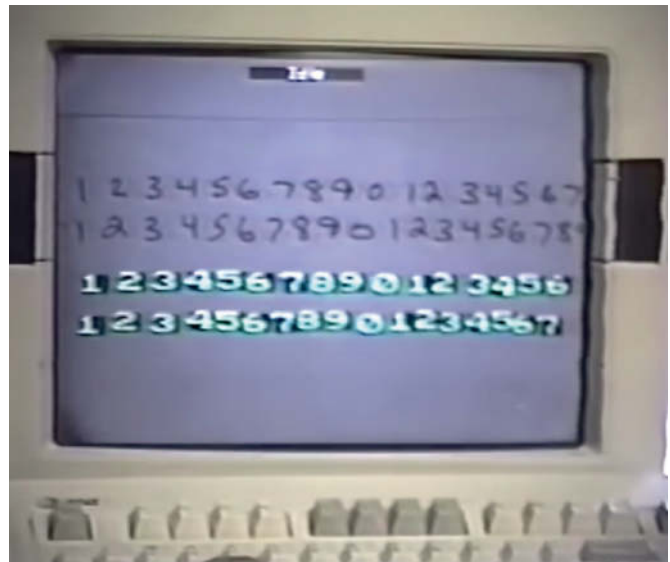


Foto: Facebook



Erste Erfolge: 1995 entwickelte LeCun für die Bell Labs ein System, das Handschrift lesen konnte.



Fotos: Facebook

Versailles mit der Suche nach wissenschaftlichen Veröffentlichungen, bevor die Forschung an Perzeptrons ausstarb.

Dann entdeckte er, dass eine kleine Gruppe von Forschern in den Vereinigten Staaten im Verborgenen begonnen hatte, weiter an neuronalen Netzen zu arbeiten. „Das war wirklich eine Untergrundbewegung“, sagt er. Um Ablehnungen beim Peer Review zu entgehen, vermieden die Forscher in ihren Aufsätzen sorgfältig den Gebrauch von Begriffen wie „neuronal“ oder „Lernen“. Nichtsdestotrotz arbeiteten sie an etwas, das Rosenblatts altem Problem, neuronale Netzwerke mit mehreren Lernstufen zu trainieren, äußerst ähnlich sah.

LeCun schloss sich dieser Untergrundbewegung an, nachdem er 1985 ihre zentralen Figuren kennengelernt hatte, darunter einen leicht verschrobenen Briten namens Geoff Hinton, der heute bei Google und der University of Toronto arbeitet. Sie wurden sofort Freunde, gegenseitige Bewunderer – und der Kern einer kleinen Gemeinde, die die Idee der neuronalen Netzwerke wiederbelebte.

Nachdem LeCun 2003 an die New York University kam, gründeten er, Hinton und ein Professor der University of Montreal namens Yoshua Bengio eine Gruppe, die LeCun heute die „Deep-Learning-Verschörung“ nennt. Um das Jahr 2010 begann Deep Learning, etablierte Techniken bei Alltagsaufgaben zu schlagen, zum Beispiel dem Klassifizieren von Bildern. Doch neuronale Netze waren den meisten Forschern noch fremd und galten weiterhin als unnütz.

2012 änderte sich das: Erstmals gelang es Hinton und zwei Doktoranden, mithilfe eines tiefen neuronalen Netzwerks die Konkurrenz beim wichtigsten Wettbewerb für Bilderkennung zu schlagen. Bei der „ImageNet Large Scale Visual Recognition Challenge“ muss die Software 1000 unterschiedlichste Objekte in verschiedenen Bildern identifizieren, von Moskitonetzen bis Moscheen. Die Software aus Toronto war um zehn Prozent besser als die des zweitplatzierten Wettbewerbers. Im Dezember

2013 verblüffte der Facebook-CEO Mark Zuckerberg die akademische Gemeinde, indem er auf der größten Forschungskonferenz für neuronale Netze zu einer Party einlud und bekannt gab, dass LeCun das Fair-Team gründen würde.

Facebooks New Yorker Büro erreicht man von LeCuns Universitätsbüro nach einem dreiminütigen Spaziergang den Broadway hinauf. Es residiert auf zwei Etagen eines Gebäudes, das im frühen 20. Jahrhundert als Kaufhaus erbaut wurde. In dem Großraumbüro sind die Arbeitsplätze dichter gepackt als in Facebooks Hauptquartier im kalifornischen Menlo Park. Trotzdem lassen es sich die Mitarbeiter nicht nehmen, auf lenkbaren Skateboards unterwegs zu sein. Ausgehängte Zettel laden zu einem wöchentlichen Trinkspiel mit Bier und Pingpong-Bällen ein. Fast die Hälfte von LeCuns Team aus führenden KI-Forschern arbeitet hier, der Rest auf Facebooks kalifornischem Campus oder in einem Pariser Büro. „Ich habe alle Leute aus diesem Bereich eingestellt, die ich kriegen konnte“, sagt LeCun.

Ein neuronales Netzwerk „lernt“, Sprache zu verstehen, indem es Sätze Wort für Wort durcharbeitet und für jedes Wort berechnet, wie wahrscheinlich es im Zusammenhang mit dem vorhergehenden oder nächsten Wort auftritt. Die Software repräsentiert jedes Wort als einen Vektor – eine Reihe von Zahlen –, der seine Beziehung zu anderen Worten anzeigt. Dieses Verfahren kann frappierend genau sprachliche Konzepte erfassen. Der Unterschied zwischen den Vektoren für „König“ und „Königin“ ist zum Beispiel der gleiche wie für „Mann“ und „Frau“. Die Vektoren für „Papier“ und „Pappe“ liegen nahe beieinander, die für „Sofa“ und „Couch“ sogar noch näher. Der gleiche Ansatz funktioniert für ganze Sätze. Hinton nennt das „Gedankenvektoren erzeugen“. Google möchte das nutzen, um seine automatische Übersetzung zu verbessern. Ein kürzlich erschienener Aufsatz von Forschern einer chinesischen Universität und Microsofts Peking Labor beschreibt eine Version der Vektortechnik, die manche Menschen bei Fragen aus Intelligenztests schlägt.

LeCuns Gruppe arbeitet jedoch bereits an den nächsten Schritten. „Sprache an sich ist nicht so kompliziert“, sagt er. „Kompliziert ist die Kombination aus einem tiefen Verständnis für Sprache und dem Weltwissen, das uns den gesunden Menschenverstand verleiht.“ Die Facebook-Forscher erfanden ein Deep-Learning-System, das erste Anzeichen für eine Art Mutterwitz zeigt. Die Technik nennen sie Memory Network.

Ein Memory Network ist ein neuronales Netz mit einem angedockten Speicher, der gelernte Fakten so ablegt, dass sie sich nicht jedes Mal löschen, wenn frische Daten hereinkommen. Facebooks KI-Labor hat Versionen entwickelt, die über das nötige Wissen verfügen, um einfache Fragen zu Texten zu beantworten, die sie noch nie zuvor gesehen haben. Ihren rudimentären gesunden Menschenverstand erwarb die Software, indem die Forscher sie gewissermaßen zur Schule schickten: Sie gingen Schritt für Schritt Texte mit einer einfachen Handlung durch und verrieten der Software, welche Antwort zu welcher Frage passt.

Als die Forscher dem Memory Network zum Beispiel eine stark simplifizierte Zusammenfassung des Buchs „Herr der Ringe“ präsentierten, konnte es Fragen wie „Wo ist der Ring?“ und „Wo war Frodo, bevor er zum Schicksalsberg kam?“ beantworten.

Im nächsten Schritt will LeCun die Software komplexeren Texten aussetzen. Schließlich soll sie irgendwann einen nützlichen virtuellen Assistenten abgeben, und das Leben ist nun einmal komplizierter als eine Zusammenfassung von „Herr der Ringe“. Das nötige Unterrichtsmaterial könnte eine virtuelle Concierge liefern, die Facebook demnächst vorstellen wird. Sie heißt Moneypenny und soll Nutzern bei Aufgaben wie einer Tischreservierung im Restaurant helfen – zunächst unterstützt von menschlichen Hotline-Mitarbeitern. LeCuns Team könnte sein Memory Network über Moneypennys Schulter schauen lassen, bevor es schließlich Erfahrungen durch die Interaktion mit den Menschen selbst machen würde.

Die Herausforderung ist riesig: Bisher schaffen neuronale Netze nur sehr einfache Schlussfolgerungen. Auch die Fähigkeit, Pläne zu schmieden, geht ihnen völlig ab, gibt LeCun zu. Der Schritt hin zu einem System, das Unterhaltung führen kann – und sei das Thema noch so eng umgrenzt –, erfordert erhebliche Anstrengungen. Doch die Resultate aus der bisherigen Arbeit mit der Technik machen LeCun zuversichtlich. „Die Revolution ist auf dem Weg“, sagt er.

Andere sind sich da nicht so sicher. Deep-Learning-Software habe bisher nur die einfachsten Funktionen für das demonstriert, was wir als Gespräch akzeptieren würden, sagt Oren Etzioni, Geschäftsführer des Allen Institute for Artificial Intelligence in Seattle. Die noch benötigten Kapazitäten für Logik und Planung, sagt er, unterscheiden sich stark von dem, was neuronale Netze bisher am besten tun: Sequenzen von Pixeln oder akustischen Wellenformen zu verdauen und zu entscheiden, welche Kate-



gorie von Bild oder Wort sie repräsentieren. „Die Probleme des Verstehens natürlicher Sprache sind nicht auf die gleiche Weise reduzierbar“, sagt er.

Facebooks Lenker wissen, dass LeCuns Gruppe noch weit entfernt von einer Software ist, mit der sich Menschen unterhalten können. Mike Schroepfer, Technischer Direktor des Unternehmens, denkt trotzdem schon einmal darüber nach, wie sie sich einsetzen ließe. „Mit einem System, das Sprache auf einer höheren Ebene versteht, kann man ganz anders interagieren“, sagt er. Denkbar wäre beispielsweise, dass man die Software so einstellt, dass sie einem zwar die neuesten Babyfotos eines Freundes anzeigt – nicht aber dessen Witze, weil man seinen Humor nicht mag. Dazu müsste das Programm aber erkennen, was ein Witz ist. „Ich glaube, eine derartige Version ist in naher Zukunft durchaus realisierbar“, sagt er.

Die für solche Interaktionen nötigen Algorithmen würden auch die Filter verbessern, mit denen das Unternehmen seinen Nutzern vermeintlich relevante Beiträge und Anzeigen präsentiert. Und sie könnten entscheidend für Facebooks Ambitionen sein, mehr zu werden als nur ein Ort, an dem man Kontakte knüpft. Zurzeit beginnt Facebook zum Beispiel, Artikel und Videos für Medien- und Unterhaltungsunternehmen zu hosten. Dafür wird es den Nutzern bessere Möglichkeiten anbieten müssen, Informationen zu managen. Virtuelle Assistenten und andere Anwendungen für LeCuns Arbeit könnten auch weitere ehrgeizige Aktivitäten von Facebook unterstützen. Die Oculus-Gruppe etwa arbeitet daran, die virtuelle Realität in den Massenmarkt zu bringen.

LeCun vermutet, virtuelle Helfer mit einer bis dato beispiellosen Sprachbeherrschung könnten in zwei bis fünf Jahren verfügbar sein. Er erwartet, dass die Deep-Learning-Technologie ihre Kritiker erneut widerlegt – diesmal beim Sprachvermögen. „Es ist das gleiche Phänomen, das wir vor 2012 beobachteten“, sagt er. „Die Dinge beginnen zu funktionieren, aber die Vertreter der eher klassischen Technik sind nicht überzeugt. Innerhalb von ein oder zwei Jahren wird sich das radikal ändern.“ ☘



HORIZONTE
GENTECHNIK

Die nächste große Gen-Debatte

Illustration: Laurie Bollitt

Der US-Agrochemiekonzern Monsanto will Pflanzen per RNA-Sprays resistent machen gegen Pflanzenschutzmittel oder Insektenbefall, ohne ihre Gene selbst zu verändern. Die Methode **schaltet Gene indirekt ab**. Wie wirksam und sicher ist sie?

VON ANTONIO REGALADO



Kartoffelkäfer sind gegen 60 Gifte resistent.

Der Kartoffelkäfer ist ein unersättlicher Vielfraß. Er zerlegt zehn Quadratzentimeter Blatt pro Tag und kann komplette Pflanzen entlauben. Doch die Käfer in Monsantos Laboren nahe St. Louis, die sich durch eine leuchtend grüne und sorgfältig mit einem Netz bedeckte Pflanze füttern, sind dem Untergang geweiht. „Ich bin ziemlich sicher, dass 99 Prozent von ihnen bald tot sein werden“, sagt Jodi Beattie, eine Monsanto-Forscherin. Der Grund ist ein RNA-Molekül, die Arbeitskopie eines Genabschnitts auf der DNA. Mit ihm besprühten die Forscher die Pflanzen. Was zunächst harmlos klingt, hat es in Wahrheit in sich: Die Erbgutkopie löst in den Käfern einen Mechanismus namens RNA-Interferenz (RNAi) aus. Er deaktiviert vorübergehend ausgewählte Gene: In diesem Fall schalteten die Forscher eins ab, das für die Käfer lebenswichtig ist.

Der Reiz solcher Sprays – Monsanto nennt sie BioDirect – liegt darin, die Gene einer Pflanze zu beeinflussen, ohne das Genom direkt zu verändern und zulassungspflichtige gentechnisch veränderte Organismen zu erzeugen. Monsanto hofft, auf diese Weise den Kontroversen um GM-Pflanzen zu entgehen. Denn RNA-Moleküle finden sich überall in der Nahrung, ihr Verzehr gilt bisher für Menschen als nicht giftiger als ein Glas Orangensaft. Die Sprays lassen sich darüber hinaus je nach Bedarf schnell zuschneiden: auf einen Insektenbefall oder eine neue Art von Virus. Sie sollen präzise genug sein, um nur Kartoffelkäfer zu töten, nicht aber etwa Marienkäfer.

Ob die Zulassungsbehörden diese Meinung teilen, ist keineswegs garantiert. Nach Auskunft des Bundesamts für Verbraucherschutz und Lebensmittelsicherheit (BVL) würden derartige Pflanzen zwar nicht als genetisch verändert gelten. Als was dann, ist jedoch unklar. RNA-Produkte seien nicht durch die aktuellen Anforderungen für Pflanzenschutzmittel erfasst. Für sie müssten dem BVL zufolge also auf EU-Ebene die Zulassungsbestimmungen angepasst werden. Die Bühne für die nächste große Gen-Debatte ist bereitet.

Die sogenannte RNA-Interferenz ist ursprünglich ein natürlicher Mechanismus. Er scheint sich sowohl bei Tieren als auch Pflanzen als Abwehrsystem gegen Viren entwickelt zu haben und wird ausgelöst, wenn eine Zelle auf fremde doppelsträngige RNA trifft. Diese erzeugen zum Beispiel Viren, wenn sie versuchen, ihr genetisches Material in der Zielzelle zu kopieren. Die Zelle wehrt sich, indem sie die Moleküle zerhackt und mithilfe der Bruchstücke – wie mit einem Fahndungsfoto – weiter Jagd auf RNA-Abschnitte macht, die diese Stückchen enthalten.

Der Mechanismus lässt sich jedoch auch gegen seinen Schöpfer richten. Denn höher entwickelte Zellen nutzen RNA als Post-

boten, um Bauanleitungen für Hormone oder Enzyme an die Zellmaschinerie zu übermitteln. Schleusen Forscher nun einen auf ein Gen zugeschnittenen RNA-Doppelstrang ein, der mit bestimmten Postboten identisch ist, werden diese abgefangen. Das zugehörige Gen ist lahmgelegt (siehe Grafik auf S. 48).

Auch die Agrargrößen Bayer und Syngenta forschen an derartigen genetischen Sprays. 2012 etwa zahlte Syngenta 523 Millionen Dollar für Devgen, ein europäisches Biotech-Unternehmen, mit dem es an RNA-Insektiziden zusammengearbeitet hatte. Beide Unternehmen wollen ihre Programme jedoch nicht öffentlich kommentieren.

Monsanto dagegen schon. Drei Anwendungsbereiche untersuchen die Forscher derzeit. Zum einen setzen sie auf RNA-Sprays gegen den Kartoffelkäfer, der bereits gegen mehr als 60 herkömmliche Insektizide einschließlich DDT resistent geworden ist. Der Angriff mittels RNA-Interferenz dagegen werde schwer zu überwinden sein, glaubt Jeremy Williams, der das Insektizid-Programm leitet. Sollte der Käfer eine Resistenz gegen das RNA-Molekül entwickeln, könnten Genetiker „die Sequenz um ein paar Buchstaben verschieben“ oder mehrere Gene gleichzeitig aufs Korn nehmen.

Monsanto-Forscherin Jodi Beattie deutet auf ein großes Glasgefäß, in dem getrocknete, gereinigte RNA glänzt wie Styropor-Verpackungschips. Vor ein paar Jahren hätte diese Menge noch eine Million Dollar gekostet, jetzt sind es etwa 50 statt 25 000 Dollar pro Gramm. Ein Zehntel davon reicht laut der Firma aus, um alle Käfer auf einem knappen halben Hektar Anbaufläche zu töten. Das Produkt gegen Kartoffelkäfer könnte 2020 auf den Markt kommen, sagt Projektleiter Williams. Monsanto versucht derzeit noch, das Spray regenfest zu machen, damit es mindestens eine Woche an den Blättern haftet.

Zum Zweiten will Monsanto mit den RNA-Sprays seinem Unkrautvernichtungsmittel Glyphosat – Markenname Roundup – neues Leben einhauchen. Der Monsanto-Chemiker Doug Sammons forscht zu diesem Zweck an Unkräutern, die resistent gegen Glyphosat sind. Sein Ziel: Jene Erbgutabschnitte zu identifizieren, die für die Unempfindlichkeit verantwortlich sind – und sie auszuschalten. Das gelang. Eine Mischung von Roundup mit der passenden Doppelstrang-RNA ließ die resistenten Unkräuter in Labor- und Feldtests eingehen. Einige Pflanzenexperten sind von der Wirkung der Sprays allerdings nicht überzeugt. Stephen Powles, Direktor der australischen Herbizidresistenz-Initiative, vermochte Monsantos Unkraut-Experiment nicht zu wiederholen. „Doppelsträngige RNA in Pflanzen einzubringen ist in Wahrheit sehr schwierig“, sagt er. Und der renommierte Pflanzenbiologe Richard Jorgensen, der als einer der Ersten



RNA-Interferenz bei Pflanzen beobachtet hat, hält das Modifizieren von Pflanzeigenschaften per Spray „potenziell für Flickwerk“. „Möchten Sie wöchentlich sprühen und dann hoffen, dass es in jeder Zelle ankommt?“, fragt er.

Zum Dritten will Monsanto nicht nur auf der Pflanzenoberfläche bleiben, sondern die RNA-Insektizide in die Zellen einbauen. Erste Experimente laufen für den Kampf gegen die Zitruspest. Sie verursacht in Florida jährlich Schäden in dreistelliger Millionenhöhe. Ursache ist ein von asiatischen Blattflöhen übertragenes Bakterium. Es verfärbt die Orangen, macht sie hart, und ihr Saft schmeckt wie Kerosin. Monsanto arbeitet mit dem Insektenexperten Wayne Hunter im Forschungslabor des US-Landwirtschaftsministeriums in Fort Pierce zusammen.

Hunter trankte die Wurzeln der Orangenbäume mit RNA oder injizierte sie in die Stämme, um die Bakterienüberträger zu treffen und lebenswichtige Gene der Insekten abzuschalten. Seine bisherigen Versuche zeigen jedoch, dass RNA-Behandlungen für Orangenhaine bestenfalls ergänzend geeignet sind. Im Labor starben die Insekten erst nach vier Tagen. Einige überlebten zwei Wochen. In einer Feldstudie blieben die Bäume mit Blattflöhen bedeckt – ob es sich aber um neu hinzugeflogene Exemplare handelte, ist unklar.

Alle drei Ansätze bergen Konfliktpotenzial. Glyphosat etwa gilt mittlerweile offiziell als gesundheitsbedenklich. Die Internationale Agentur für Krebsforschung, eine Untergruppe der Weltgesundheitsorganisation, hat es im März 2015 als „wahrscheinlich“ krebserregend eingestuft. Es nun in neuer Formel auf den Markt zu bringen, dürfte Widerstand auslösen. Aber auch die RNA-Pestizide selbst könnten Ängste wecken. Schon Monsanto's eigene Entdeckungen unterstreichen, dass doppelsträngige RNA von Organismus zu Organismus wandern kann. Genau das war schließlich der Hintergrund von Hunters Tests, Zitrusfrüchte gegen Bakterien einer Blattlaus zu impfen. RNA mag natürlich sein. Das Versprühen großer Mengen spezialisierter RNA-Moleküle in der Umwelt ist es nicht.

Monsanto bereitet sich bereits auf die unvermeidliche Sicherheitsdebatte vor. Damit die verwendete RNA keine Gene nützlicher Insekten wie Honigbienen abschaltet, sichteteten die Forscher bei den Orangenbaum-Experimenten vor der Auswahl der Zielsequenz Online-Archive mit DNA-Daten. Um zu testen, ob die synthetische RNA nicht doch unerwünschte Arten wie Bienen, Blattläuse und Mottenschildläuse schädigt, folgten Fütterversuche. Monsanto zufolge wirken die Blattfloh-Sequenzen in der Regel nur bei engen Verwandten derselben Gattung.

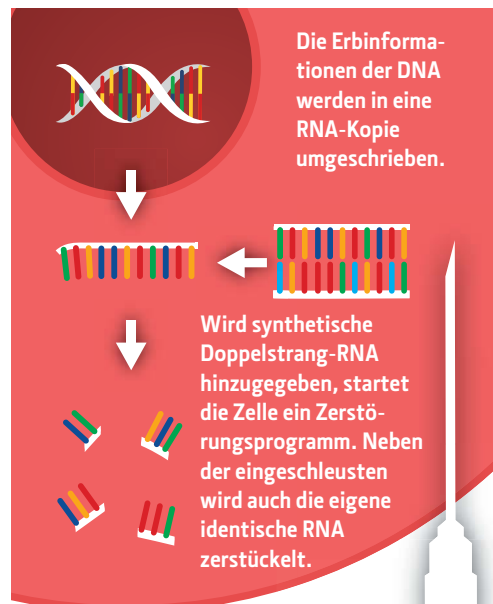
Dagegen töten herkömmliche Insektizide wahllos auch nützliche Insekten. Der Einsatz von Imidacloprid etwa wurde in Europa nach Hinweisen auf die Gefährdung von Bienenvölkern stark eingeschränkt. Zusätzlich untersuchten Mitarbeiter mögliche Auswirkungen für den Menschen. Sie analysierten Obst und Gemüse aus Geschäften, das von Pflanzenviren befallen schien, und fanden viele virale RNA-Fragmente, die hohe Übereinstimmungen mit menschlichen Genen aufwiesen. Trotzdem gebe es keinen bekannten Fall, bei dem jemand durch RNA zu Schaden gekommen wäre, so Monsanto. Es schließt daraus, dass bloße Übereinstimmung zwischen RNA-Triggern und menschlichen Genen „nur geringe biologische Relevanz“ habe.

Doch statt unabhängigen

Tests über die Sicherheit von RNA-Sprays zuzustimmen, versucht Monsanto, auf das Regelwerk selbst Einfluss zu nehmen. 2014 argumentierte der Konzern gegenüber der US-Umweltschutzbehörde EPA, die über die Regulierung von RNA-Insektiziden beraten sollte: Den Produkten sollten irrelevante Sicherheitstests erspart bleiben, inklusive Allergietests, da nur Proteine Allergien verursachen. Monsanto will auch nicht testen, ob RNA giftig für Nagetiere ist oder dauerhaft in der Umwelt verbleibt. Bei eigenen Tests habe sich auf den Boden gegossene RNA zersetzt und sei nach 48 Stunden nicht mehr nachweisbar gewesen.

Die EPA-Berater stimmten zwar zu, dass es tatsächlich wenig Hinweise auf eine Gefährdung von Menschen durch RNA-Verzehr gebe. Allerdings sahen sie weiteren Untersuchungsbedarf für „potenziell unbeabsichtigte“ ökologische Auswirkungen. Das National Honey Bee Advisory Board etwa hat darauf hingewiesen, dass die Genome vieler Insekten noch nicht bekannt seien, sodass Forscher sie nicht mit

RNA-Zielen abgleichen können. Zum anderen dürfte Nicht-Biologen das Argument, dass RNAi-Sprays das Genom der Pflanzen nicht verändern, nicht reichen. Sie werden sie trotzdem als Genpflanzen wahrnehmen. „Die Leute werden sagen, sie versprühen die RNA einfach in der freien Natur“, sagt Kassim Al-Khatib, Pflanzenphysiologe an der University of California in Davis. Und er ergänzt: „Es muss eine generelle Akzeptanz gegeben sein, bevor man einen neuen Ansatz etabliert.“ Firmeneigene Untersuchungen allein dürften da nicht reichen. ☹



RNA-Interferenz

Gene lassen sich durch fremde synthetische RNA-Stücke abschalten. Diese unterbrechen die Weitergabe der Erbinformationen von der DNA über die RNA zum Proteinbau. Die ursprüngliche DNA wird dadurch nicht verändert.

DENKEN SIE WEITER.



3 Ausgaben Technology Review mit 34% Rabatt testen und Geschenk erhalten.

IHRE VORTEILE ALS ABONNENT:

- **VORSPRUNG GENIESSEN.**
Früher bei Ihnen als im Handel erhältlich.
- **PREISVORTEIL SICHERN.**
Mehr als 34 % Ersparnis im Vergleich zum Einzelkauf während des Testzeitraums.

WÄHLEN SIE IHR GESCHENK!

Zum Beispiel:
koziol Kaffeebereiter

GRATIS

Mit UNPLUGGED von Koziol wird die Kaffeezubereitung wieder richtig zelebriert und jede Tasse kann nach eigenem Gusto zubereitet werden.



JETZT AUCH KOMPLETT DIGITAL:

- Bequem auf Ihrem Tablet oder Smartphone
- Für Android, iOS oder Kindle Fire

Jetzt bestellen und von allen Vorteilen profitieren:

WWW.TRVORTEIL.DE



Billige Kopien von Gentech-Pflanzen

Monsanto verliert das Monopol auf das erste Roundup-Ready-Saatgut. Unis stehen mit Nachahmern in den Startlöchern – und könnten eine zweite **Ausbreitungswelle der umstrittenen Technologie** lostreten.

VON ANTONIO REGALADO

Billy Maddox hat in Arkansas dieses Jahr 40,5 Hektar Land mit Sojabohnen der Sorte „Roundup Ready“ bepflanzt. Als Saatguthändler sei er eigentlich auf konventionelle Sorten spezialisiert, erzählt Maddox im gedehnten Akzent der Südstaatler. Doch dieses Jahr verkaufte er erstmals ein gentechnisch modifiziertes (GM) Saatgut. Ähnlich wie die gleichnamige, vom Agrotechnik-Konzern

Monsanto entwickelte Sorte kann sie dem Unkrautvernichtungsmittel Glyphosat (Markenname Roundup) widerstehen. Maddox musste für sie keinen Cent an Monsanto zahlen. Die Universität von Arkansas hat sie im Rahmen des „Crop Variety Improvement Program“ entwickelt – und zwar völlig legal.

Denn einige von Monsantos frühen GM-Patenten beginnen auszulaufen. Die Roundup-Ready-Schutzfrist endete bereits im vergangenen Jahr. Daher kommen die ersten „generischen GMOs“ auf den Markt – patentfreie Sorten, die nur die Hälfte kosten und deren Samen Landwirte selbst sammeln und Jahr für Jahr neu anbauen dürfen. Die umstrittene Technologie könnte damit vor einer weiteren Ausbreitungswelle stehen.

Wie im Arzneimittelmarkt könnten Unternehmen billige Generika-Samen produzieren und Marktanteile an sich reißen. Es ist noch zu früh zu sagen, ob das Gleiche bei GM-Pflanzen geschehen wird. „Wir haben Anrufe aus dem ganzen Land erhalten, aber wie groß sich das entwickelt, wissen wir noch nicht“, sagt Donald Dombek, Direktor des Crop Variety Improvement Program. Der amerikanische GMO-Markt jedenfalls könnte Konkurrenz gut gebrauchen: Mehr als 90 Prozent der in den USA angebauten Sojabohnen enthalten Monsantos Roundup-Resistenzgene.

Züchtungsspezialisten von der Universität Arkansas etwa nutzen Monsantos ehemals geschützte Technologie, um das Roundup-Resistenzgen auf eine andere Sojabohnensorte zu übertragen. Pengyin Chen kreuzte dazu jahrelang Pflanzen. Die auf diesem Weg entstandene Sorte heißt „UA5414RR“. Bisher hat die Universität 2400 Säcke davon verkauft – hauptsächlich an Händler, die die Samen vermehren. Jeder Sack enthält ausreichend Saatgut, um fast einen halben Hektar zu bepflanzen. Chen sagt, er habe die neue Sorte erschaffen, um Landwirten eine Alternative zu

bieten. Die müssen sparen – der Marktpreis für Sojabohnen ist auf einem Vier-Jahres-Tief. Die Arkansas-Samen kosten 25 Dollar pro Sack, halb so viel wie Monsantos neuere Sorten. Die Universität von Arkansas plant zwar ein Patent auf die neue Sojasorte – man werde Landwirte aber nicht davon abhalten, Samen zu sammeln. Der Marktanteil der Arkansas-Samen ist derzeit noch winzig. Doch auch andere landwirtschaftliche Hochschulen züchten eigene Generika, unter anderem in Kansas und Georgia. Die Universität von Missouri, quasi in Monsantos Hinterhof, entwickelt vier Nachzüchtungen, die noch dieses Jahr in den Handel gelangen sollen.

Monsanto gibt sich unbesorgt über das Ende der Schutzrechte. Seine neue Sojabohnen-Version „Roundup Ready 2“ habe bessere Eigenschaften und sei noch patentgeschützt. Eine dritte Generation warte bereits auf die Zulassung. Große Saatgut-Unternehmen stellen derzeit auf Roundup Ready 2 um. Probleme der älteren Sorte, warnen sie, hätten zu niedrigeren Erträgen geführt. Die Hochschulorte seien daher nicht konkurrenzfähig. Chen widerspricht: „Ich finde, sie funktioniert nach wie vor.“

Könnten die Gen-Generika damit auch nach Deutschland kommen? Monsantos Roundup-Ready-Sojabohne jedenfalls darf als Lebens- und Futtermittel importiert werden. Sollten die Nachahmerpflanzen jedoch keine exakten Kopien sein, sondern etwa die eingefügten Gene an anderer Stelle im Genom tragen, müssten diese Pflanzen „ein neues, vollständiges Zulassungsverfahren durchlaufen“, so das Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL). Sie könnten vorher nicht legal importiert werden. Der Anbau ist ohnehin untersagt, daran ändert auch das abgelaufene Patent nichts. ❖



Foto: Fotolia

Für Monsantos GM-Sojabohnen gibt es Nachahmer-Produkte.

Im ADT - Bundesverband Deutscher Innovations-, Technologie- und Gründerzentren e.V. - sind rund 160 Innovationszentren vereint, die es sich zur Aufgabe gemacht haben, Existenzgründungen zu fördern und neue, innovative Technologiefirmen zu unterstützen. Die Mitgliedszentren des ADT nehmen gründungswillige Unternehmer gern auf, beraten sie qualifiziert in allen die Unternehmensgründung betreffenden Fragen, betreuen sie bei den ersten Schritten und bieten ihnen eine hervorragende Infrastruktur – vom Büroservice bis hin zu modernsten Kommunikationsmöglichkeiten. Der Verband vertritt in erster Linie die Interessen der Mitglieder gegenüber Öffentlichkeit, Politik und Wirtschaft. Darüber hinaus bietet er den Mitgliedern neben Erfahrungsaustausch, Know-How-Vermittlung sowie nationale und internationale Netzwerke weitere Vorteile und Unterstützung.



Schutz vor Lauschangriff und Datenklau

Adlershofer IT-Spezialisten sorgen für sichere Daten

Sind Stromnetze, Flughäfen und Rechenzentren noch sicher? Wer schützt Maschinenparks und Konstruktionsdaten der Industrie? Auch ungeschützte Telefongespräche stellen ein Risiko dar. Im Technologiepark Berlin Adlershof arbeiten IT-Spezialisten wie die Rohde & Schwarz SIT GmbH, sector red und der deutsche Ableger der Zoral Labs am Schutz sicherheitsrelevanter Infrastruktur und sensibler Daten.

Ein Spezialist im Bereich Verschlüsselungssysteme ist die Rohde & Schwarz SIT GmbH. 80 Mathematiker, Informatiker und Ingenieure sorgen hier dafür, dass Daten sicher übertragen und gespeichert werden. Die Aufträge kommen von Regierungen und Militär, und zunehmend auch von Unternehmen. Denn der Schaden, den Unternehmen in Deutschland durch Industriespionage und Hackerattacken erleiden, liegt jährlich im zweistelligen Milliarden-Euro-Bereich. Viel zu tun also für die Kryptologen von Rohde und Schwarz SIT, die den weltweit ersten Verschlüsseler mit 40 Gigabit Datendurchsatz pro Sekunde zu ihren technischen Flaggschiffen zählen. Installieren IT-Dienstleister oder Banken ihn in ihre Server-Racks, verlassen Daten ihre Standorte als Rauschen. Erst nachdem der Weg durch das öffentliche Netz geschafft ist, folgt die Entschlüsselung in einem zweiten Gerät. Das Ver- und Entschlüsseln verzögert den Transfer trotz der gigantischen Datenrate nur um drei Mikrosekunden.

Mit der R&S SITGate hat das Unternehmen in diesem Frühjahr eine neuartige Firewall vorgestellt, die jede Datentransaktion kritisch beäugt und nur komplett validierte und verstandene Daten durchlässt. Bekannt ist Rohde & Schwarz SIT auch für seine Lösungen für abhörsicheres mobiles Telefonieren. Bei diesen sprechen die Gesprächspartner in kleine Geräte, die das Gesagte verschlüsseln und per Bluetooth an ihre Smartphones übertragen. Erst im Gerät am Ohr des Gegenübers folgt die Entschlüsselung.

Auch die sector red GmbH und die Zoral GmbH, beide nur einen Steinwurf von Rohde & Schwarz SIT entfernt, beschäftigen sich mit IT-Sicherheit. Das sechsköpfige sector red-Informatikerteam um Patrick Rebstein und Kerstin Vallentin berät vor allem Unternehmen aus Finanz- und Energiewirtschaft sowie im öffentlichen Sektor. „Wir analysieren branchenspezifische Spezialexsysteme, klären, welchen Schutz unsere Kunden konkret brauchen und machen uns dann an die Umsetzung“, erklärt Rebstein. Meist baue man dabei auf freier Software auf, passe diese an die Kundensysteme an und entwickle so individuellen Schutz gegen Angriffe und Datenverluste. Alan Hambrook kam im Herbst 2014 mit seiner Zoral GmbH nach Adlershof. Der Seriengründer hat seit 1981 diverse Softwarefirmen aufgebaut und will hier nun einen Forschungs- und Entwicklungsstandort seiner



sector red und Zoral Labs sind Mieter im Adlershofer Zentrum für Informations- und Medientechnologie (ZIM 3)

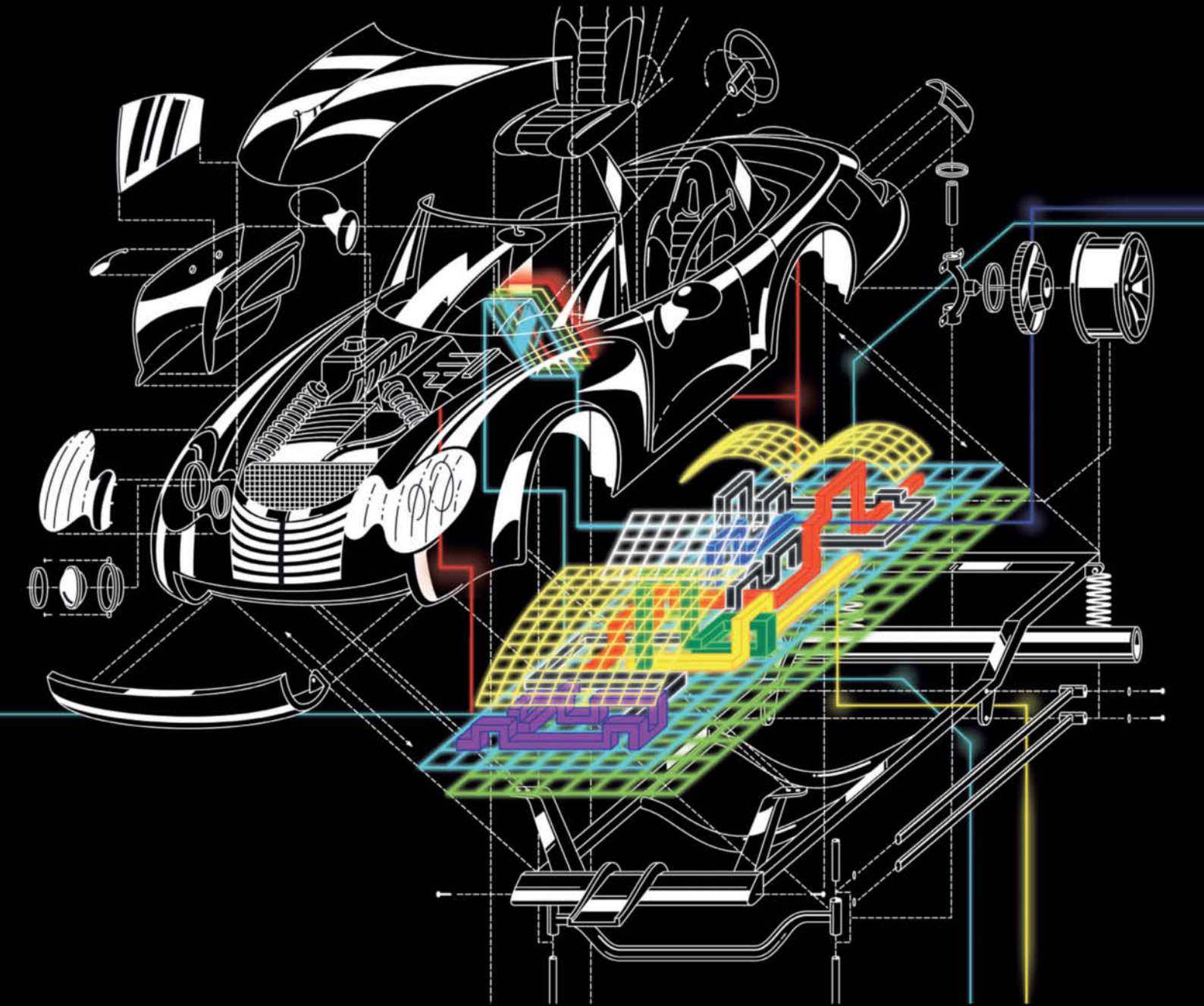
Zoral Labs etablieren. Das US-Unternehmen verbindet Künstliche Intelligenz (KI), Machine-Learning und IT-Sicherheit. Weltweit hält es Cyber-Kriminelle von Kreditkarten-, Bank- und Börsentransaktionen fern und sichert Firmennetzwerke von Technologiekonzernen mit tausenden PCs und Cloud-Anbindung. Zudem ist Zoral auf gründliche Reinigung und Wiederherstellung von Rechnern spezialisiert, die von Malware und Viren befallen waren. Dabei nutzen die Amerikaner unter anderem ihr KI-Wissen, um in fortlaufenden, automatisierten Analysen Verhaltensmuster legitimer Nutzer zu erkennen. Sobald ungebetene Gäste IT-Systeme auskundschaften, und sich dabei in ihrem Verhalten von der Masse der Nutzer unterscheiden, lösen Zorals virtuelle Alarmanlagen aus.

Rohde & Schwarz SIT, sector red und Zoral Labs – das sind drei von rund 80 IT- und Medienunternehmen am Wissenschafts-, Wirtschafts- und Medienstandort Berlin Adlershof plus der Institute für Informatik, Mathematik, Psychologie und Geographie der Humboldt-Universität, die das Thema IT-Sicherheit weiter vorantreiben werden.

Berlin Adlershof
www.adlershof.de

ADT e.V.

ADT - Bundesverband Deutscher Innovations-, Technologie- und Gründerzentren e.V.,
Jägerstraße 67, D-10117 Berlin, Tel.: 030/3920 0581, Fax: 030/3920 0582, adt@adt-online.de, www.adt-online.de



Neustart auf vier Rädern

Die Fahrzeughersteller, Apple und Google liefern sich ein **Wettrennen um das Betriebssystem fürs Auto.**

VON WILL KNIGHT

Wohin möchtest du?“, fragt Siri. Es war ein sonniger, verträumter Vormittag im Silicon Valley. Ich sitze auf dem Beifahrersitz eines Hyundai Sonata. Er kommt mir eigentlich ganz normal vor – abgesehen von den Apple-Symbolen auf dem Bildschirm und der emotionslosen Stimme von Apples virtueller Assistentin Siri, die aus den Lautsprechern dringt. Ich frage sie nach einem nahe gelegenen Sushi-Restaurant. Sie liest mir einige Läden vor, wartet auf meine Auswahl und zeigt mir dann auf dem Bildschirm den Weg.

Der Hyundai ist eines der ersten Serienfahrzeuge, die Apples Software „CarPlay“ unterstützen. Sie überträgt die Inhalte eines per Kabel angeschlossenen iPhones ans Auto. Die meisten anderen Hersteller wollen nachziehen. Zwar haben praktisch alle Autohersteller auch ihre eigenen Infotainment-Systeme mit eigenen Bedienkonzepten und eigenen Apps, aber viele Autofahrer

nutzen lieber das vertraute Smartphone. Also kaufen sie zu einem neuen Auto auch noch gleich einen Saugnapf für fünf Dollar dazu, kleben das Gerät an die Windschutzscheibe und fingern während der Fahrt daran herum. Eine wenig befriedigende Lösung: Bei meinem Mietwagen fiel es auf dem Weg vom Flughafen mehrmals ab und verschwand unter dem Beifahrersitz. Laut National Safety Council hängen mehr als 25 Prozent aller Verkehrsunfälle in den USA mit der Nutzung von Mobiltelefonen zusammen.

CarPlay lenkt deutlich weniger ab. Aufgerufen über einen Knopf am Lenkrad, kann ich mit Siri problemlos SMS versenden, telefonieren und Ziele in das Navi eingeben. Das Gleiche gilt auch für Googles Konkurrenzprodukt Android Auto, wie ich bei einer Fahrt mit einem anderen Hyundai Sonata feststelle. Google-Produktmanager Daniel Holle verbindet sein Nexus-Smartphone per Kabel mit dem Auto, und sofort gehört dessen Touchscreen der Assistenz-App „Google Now“, die aktuelle Empfehlungen auf Basis von Positionsdaten, Suchanfragen oder Mails gibt. In unserem Fall zeigt sie den Weg zur nächsten Starbucks-Filiale an, weil Holle kurz zuvor im Web

nach einem Café gesucht hat. Hätte er ein Ticket für einen baldigen Flug in seinem Postfach, erklärt mir Holle, stünde nun der Weg zum Flughafen auf dem Schirm. „Zu guten Teilen machen wir das wegen der Fahrsicherheit“, sagt er. „Aber zugleich gibt es eine enorme Chance, digitale Erfahrungen im Auto zu ermöglichen.“ (Natürlich haben solche Systeme auch ihre Grenzen: Wenn das Smartphone seine Verbindung verliert oder die Batterien leer sind, geht nichts mehr. Und die Sprachassistenten verstehen mich nicht immer richtig.)

Neue Autos rollen heute mit 50 bis 100 Computern vom Band, auf denen Millionen Zeilen Programmcode laufen. Ihre Rechenleistung nimmt laufend zu. Im Februar hat der ameri-

» **Apple und Google wollen nicht mehr auf die Autobauer warten.** «

kanische Chiphersteller Nvidia zwei neue Grafikchips für Autos angekündigt: Der eine kann 3D-Grafiken für bis zu drei Displays im Auto gleichzeitig erzeugen, der andere Daten von bis zu zwölf Kameras sammeln und verarbeiten. Auf letzterem läuft selbstlernende Software, die Hindernisse auf der Straße erkennt. Die beiden Chips lassen erahnen, welche enormen Möglichkeiten moderne Autos für IT-Firmen bieten.

Noch gibt es allerdings keine Software, die – wie ein echtes Betriebssystem – umfassenden Gebrauch von all den Computern macht. Google und Apple können einstweilen nur wenige Fahrdaten nutzen. Etwa ob ein Auto vorwärts oder rückwärts fährt. Tiefere Einblicke verweigern die Autohersteller noch. Eine entscheidende Frage ist, ob sich das künftig ändern wird. Wer auch immer in Zukunft die Software für die zahlreichen Auto-Steuergeräte liefert, wird die Innovationen im Automobilbereich prägen. Wenn Apple und Google Zugriff auf die vielen Rechner im Auto bekämen, könnten sie mit ihrer Software-Kompetenz ein solches Betriebssystem für Autos schaffen.

Vielleicht ist das auch die Erklärung dafür, warum sich Apple und Google jetzt auch an Fahrzeug-Hardware versuchen: Sie



1966

1978

1981

1983

1987

1990er

Ingenieure von General Motors schlagen Funksignale und Sensoren in den Straßen als Navigationshilfe vor.

Ein Prozessor von Motorola ermöglicht einen elektronischen Tempomaten.

Motorola-Prozessoren regeln bei Maschinen von General Motors Vergaser und Einspritzpumpe.

Beim Toyota Crown wird die elektronische Stabilitätskontrolle eingeführt.

Der erste Touchscreen erscheint, an Bord des Buick Riviera.

Elektronik breitet sich weiter aus – in Sitzen, Instrumententafeln und Schlössern.

wollen den vollen Zugriff auf die Zeit von Menschen in Autos, ohne darauf zu warten, dass die klassischen Hersteller ihnen weitere Teile ihrer Fahrzeuge zugänglich machen. Google hat bereits eigene selbstfahrende Autos gebaut, die mit einer Kombination aus Sensoren, Kartendaten und intelligenter Software arbeiten. Auch Apple entwickelt offenbar ein eigenes Auto. Das Unternehmen kommentiert derartige „Gerüchte und Spekulationen“ zwar nicht. Aber es stellt gerade Dutzende Leute mit einschlägigen Kenntnissen ein. Außerdem wurden auf kalifornischen Straßen schon sensorbestückte Vans gesehen, die Apple gehören.

Die weitaus größere Chance für Apple und Google liegt allerdings darin, nicht nur die eigenen, sondern alle Autos mit Software für automatisches Fahren, fortgeschrittene Diagnostik oder drahtlose Updates zu versehen. Schon jetzt gibt es bei

Android Auto einen Knopf, der für künftige Diagnose-Apps reserviert ist. Google erwartet, dass diese Apps zunächst von den Autoherstellern selbst kommen werden. Sie sollen dann deutlich mehr Informationen liefern als die mysteriös blinkenden Motor-Warnleuchten von heute. Natürlich würde aber auch Google selbst gern auf die Autodaten zugreifen, sagt Holle. Denn dann könnte Google Now zum Beispiel einen Besuch in der nächsten Werkstatt arrangieren, wenn der Motor zu heiß wird.

Wenn sie verhindern wollen, dass Google und Apple in diese Lücke stoßen, müssen die Autohersteller sie selbst schließen. Also gründen sie Labore im Silicon Valley. Ford etwa hat in diesem Januar eine Forschungsabteilung in Palo Alto eröffnet, in direkter Nachbarschaft zu Skype und Hewlett-Packard. Sie

ist ausgestattet wie ein typisches Start-up: rote Sitzsäcke, 3D-Drucker und viele leere Tische, an denen bald über hundert Ingenieure arbeiten sollen. Ich treffe mich dort mit dem Interface-Designer Casey Feldman. Als ich komme, steht er gerade auf einem Balancierbrett vor seinem Schreibtisch und arbeitet an „Sync 3“, dem neuesten Infotainment-System von Ford. Noch läuft es mit Fords eigener Software, doch künftig will der Hersteller den Bildschirm auch CarPlay oder Android Auto überlassen. Zum Testen verwendet Feldman eine Kiste mit Touchscreen und Reglern, ungefähr so groß wie ein Mini-Kühlschrank.



Mit solchen Fahrzeugen wollen Stanford-Forscher zeigen, was geht.



1993	1995	1996	2007	2012	2013
Ein neuer internationaler Standard lässt die eingebetteten Computersysteme miteinander sprechen.	Das erste Satelliten-navigationsystem wird eingeführt: GuideStar für das Oldsmobile Eighty Eight.	Das OBD2-System wird Standard. Es ermöglicht, bestimmte Fahrzeugdaten auszulesen.	Der Volvo S80 wird mit einem Warnsystem für den toten Winkel ausgestattet.	Teslas Model S erscheint. Es hat einen 17-Zoll-Touchscreen und die Möglichkeit drahtloser Updates.	Der Infiniti Q50 ist das weltweit erste Auto mit elektronischer Steuerung.

Schon 2010 hatte Ford sein erstes eigenes Touchscreen-Interface eingeführt, genannt „MyFord Touch“. Es steckte voller Fehler, Kunden fanden es übermäßig kompliziert. Als Ford 2011 bei den Zuverlässigkeitsranglisten der Zeitschrift „Consumer Report“ vom 10. auf den 20. Platz abrutschte, galt MyFord Touch als zentrale Ursache. Als Reaktion verschickte Ford 250 000 Speichersticks mit Software-Updates an seine Kunden.

Mit Sync 3 will Ford es nun besser machen. Es kann nicht nur Apps wie Spotify oder Pandora Radio ausführen, sondern verbindet sich auch mit dem heimischen WLAN, um Patches und Updates abzurufen. „Das ist ein kultureller Wandel“, sagt Dragos Maciucă, technischer Leiter des Ford-Labors. Man wolle „einen Teil der Einstellung und Prozesse des Silicon Valley in die Autoindustrie übernehmen“, erklärt er. Das äußert sich zum Beispiel durch eine gewisse Offenheit: Ein Modul namens OpenXC ermöglicht es Entwicklern, eine Vielzahl von Sensordaten aus dem Auto abzurufen und in ihre Apps oder Anwendungen einfließen zu lassen. Ein Ford-Ingenieur hat damit beispielsweise einen Schalthebel entwickelt, der aufleuchtet oder vibriert, wenn es Zeit zum Schalten ist.

Ansonsten hat OpenXC bislang allerdings wenig bewirkt. Wenn irgendjemand Ideen für weitere Anwendungen hat, dann Chris Gerdes. Er ist Maschinenbauprofessor und leitet das Dynamic Design Lab der Stanford University. Ursprünglich wollte er in Robotik promovieren, doch nachdem er einen alten Chevy Cavalier komplett restauriert hatte, stieg sein Interesse an Autos. In seinem Labor arbeiteten Studenten in großen, offenen Arbeitsbereichen an unterschiedlichen Projekten: ein leichtes Auto mit Solarantrieb, ein handgefertigter Dünenbuggy, ein Ford Fusion voller Sensoren. Gerdes zeigt auf den Fusion. Nachdem Ford den Studenten eine spezielle Software-Schnittstelle geöffnet hatte, war es für sie relativ einfach, das Auto autonom fahren zu lassen. Der Buggy treibt die Programmierbarkeit auf die Spitze – so gut wie jede Komponente lässt

sich über einen computergesteuerten Aktuator verstellen. Die Federung jedes einzelnen Rads kann beispielsweise so angesteuert werden, dass sie eine normale Straße glatt bügeln wie eine Eisdecke.

Tesla zeigt schon im Alltag, wie bedeutend Software-Innovationen für Autohersteller werden könnten. Die Elektrolimousine Model S, auf dem Markt seit 2012, ist das wohl am stärksten computerisierte Serienauto der Welt. Es hat einen 17-Zoll-Touchscreen, eine Mobilfunkverbindung und einen Webbrowser. Fahrer können alles Mögliche am Fahrzeug einstellen, beispielsweise Federung und Beschleunigung (von „normal“ bis „irre“). Alle paar Monate bekommen sie ein Software-Update mit neuen Funktionen, etwa einen Berg-Anfahrmodus oder eine Toter-Winkel-Warnung. Für diesen Sommer hat Tesla-Chef Elon Musk ein weiteres Update angekündigt, das Modellen, die bereits mit den nötigen Sensoren ausgestattet sind, autonome Autobahnfahrten ermöglicht. Das Unternehmen mit Sitz in Palo Alto arbeitet sogar schon an einem Autopiloten, der den Wagen rechtzeitig vor die Tür fährt, wenn ein Termin im Kalender des Besitzers steht.

Wie sinnvoll Software-Updates aus der Ferne sein können, zeigte sich Ende 2013. Damals waren mehrere Model S in Flammen aufgegangen, nachdem auf der Fahrbahn herumliegender Müll ihre Batterien aufgeschlitzt hatte. Statt die Wagen zurück in die Werkstätten zu rufen, änderte Tesla per Mobilfunk die Fahrwerkseinstellung, um die Bodenfreiheit zu erhöhen.

Gleichzeitig jedoch locken solche Möglichkeiten auch Übeltäter an (siehe folgende Seite). „Niemand weiß so richtig viel über Autosicherheit und worauf es dabei eigentlich ankommt, weil es zu wenig Forschung darüber gibt“, sagte Computerexperte Charlie Miller, der bereits einen Toyota Prius und einen Jeep Cherokee gehackt hat. Stanford-Forscher Gerdes glaubt trotzdem nicht, dass Sicherheitsbedenken die Computerisierung von Autos verzögern werden: „Die entscheidende Frage ist, wie schnell man vorgehen kann, ohne auf Sicherheit zu verzichten.“ ☞

„Hört auf auf zu erzählen, dass Autos nicht hackbar sind!“

Schon vor rund fünf Jahren zeichnete sich ab, wie angreifbar digital hochgerüstete Autos sind: Im Februar 2010 ließen sich Dutzende Leasing-Autos in der Gegend um Texas plötzlich nicht mehr starten und begannen unerklärlicherweise zu hupen. Sie waren mit Geräten ausgestattet, mit denen die Leasinggesellschaft sie deaktivieren konnte, falls der Fahrer seine Raten nicht zahlte. Ein wütender Ex-Mitarbeiter nutzte seinen Zugang zum System, um sich zu rächen.

Konnte das noch als menschele Anecdote abgetan werden, ging es danach ans Eingemachte: Spezialisten vom Center for Automotive Embedded Systems Security zeigten 2011 verschiedene Wege auf, in Autos einzudringen: Über den internen Daten-Bus („CAN-Bus“), das CD-Radio, über Smartphone-Trojaner, über Mobilfunk und über die Reifendrucksensoren. Sie konnten Türen öffnen, Wegfahrsperrn abschalten, Bremsen deaktivieren oder Gespräche im Auto abhören (siehe TR 8/2012, Seite 46). Bei welchen Modellen es ihnen gelungen war, wollten die Forscher aus Sicherheitsgründen nicht mitteilen.

Oft bauen die Fahrzeugbesitzer unwissentlich noch weitere Sicherheitslücken in ihre Autos ein: Der US-Forscher Corey Thuen hat 2014 einen Telematikstecker für die OBD2-Diagnoseschnittstelle gehackt, mit dem eine US-Versicherung das Fahrverhalten ihrer Kunden erfasst. „Die Firmware kennt keine Validierung von Updates, kein sicheres Booten, keine sichere Kommunikation oder Verschlüsselung“, zitiert ihn das US-Magazin „Forbes“. „Im Grunde nutzt sie überhaupt keine Sicherheitstechnologie irgendeiner Art.“ Forschern der University of California gelang kürzlich sogar, über solche Stecker per SMS die Bremsen einer Corvette bei niedrigem Tempo abzuschalten. „Dieses Problem ist besonders ernst, weil es sich um eine Nachrüstlösung handelt, auf die Autobauer keinen Einfluss haben“, schreiben die Forscher.

Solche Hacks offenbaren eine vollkommen neue Dimension, denn bisher mussten Angreifer meist physischen Zugriff auf das Auto haben, um Schadsoftware einzuschleusen. Doch mittlerweile gelingt es ihnen immer öfter, aus der Ferne zuzuschlagen. Den bisher spektakulärsten Hack zeigten die beiden Computerexperten Charlie Miller und Chris Valasek in diesem Sommer: Sie brachten einen Jeep Cherokee aus der Ferne komplett in ihre Gewalt. Ähnliches war ihnen zwar schon früher gelungen, doch dazu mussten sie ihren Rechnern direkt an die OBD2-Schnittstelle anstöpseln. Nun konnten sie über eine Lücke im Infotainmentsystem zum CAN-Bus eines Jeep Cherokee vordringen und Bremsen, Gas, Türverriegelung, Klimaanlage und Scheibenwischer steuern. Die Fahrt mit einem eingeweihten „Wired“-Redakteur landete im Straßengraben.

Beim ersten Versuch, die Lücke zu stopfen, blamierte sich der Jeep-Hersteller Fiat Chrysler erneut: Er forderte die Kunden laut ORF auf, eine ganze Reihe von „.exe“ und „.zip“-Dateien auf ihre Privat-PCs herunterzuladen und dabei alle Warnungen des Betriebssystems zu ignorieren. Ein solches Prozedere im Jahr 2015 anzubieten sei „hochgradig dilettantisch“ und potenziell weit gefährlicher als die Sicherheitslücke selbst, sagte der österreichische Sicherheitsexperte Joe Pichlmayr. Schließlich musste Fiat Chrysler 1,4 Millionen betroffene Wagen zurück in die Werkstätten rufen. Europäische Modelle sind nach bisherigen Erkenntnissen nicht betroffen, da sie ein anderes Funkmodul nutzen.

Etwa zeitgleich entdeckte der Programmierer Samy Kamkar eine weitere Sicherheitslücke: Er schnitt im Juli 2015 die Kommunikation zwischen einem Chevrolet Volt und der App „OnStar RemoteLink“ mit. Fortan konnte er die gleichen App-Funktionen nutzen wie der Besitzer, etwa die Türen entriegeln und den Motor starten.

Deutsche Hersteller versichern gern, dass bei ihnen nicht so ein Schlendrian herrsche. Doch darauf sollten Kunden sich nicht verlassen. „OnStar RemoteLink“ will künftig auch Opel anbieten. Zudem funktioniert Kamkars Hack nach seinen Aussagen prinzipiell auch bei ähnlichen Apps von Mercedes, BMW und Viper. Zu guter Letzt wurde BMW Anfang des Jahres dabei erwischt, Daten zum Öffnen der Türen unverschlüsselt über das Mobilfunknetz zu versenden. Weltweit sind 2,2 Millionen Fahrzeuge davon betroffen.

Charlie Miller (links) und Chris Valasek präsentieren ihren Hack auf der Black-Hat-Konferenz.



Foto: David Paul Morris/Bloomberg/Getty Images

Auch die Transpondersysteme für die Kommunikation zwischen Auto und Zündschlüssel sind nicht sicher. Motorolas System Megamos wurde bereits 2012 gehackt. Die Details wurden aber erst jetzt veröffentlicht, weil Volkswagen gegen eine Offenlegung geklagt hatte. Obwohl das System von vielen Herstellern genutzt wird, ist der Fall deshalb nun allgemein als „Volkswagen-Hack“ bekannt. Die Veröffentlichung brachte unter anderem zu Tage, dass viele Wagen eine Standard-PIN benutzten, die sich innerhalb einer halben Stunde mit einem normalen Rechner durch einfaches Durchprobieren ermitteln ließ. Und das, obwohl die Mehrkosten für ein sichereres System laut Heise Autos bei unter einem Dollar pro Schlüssel liegen.

Viele dieser Hacks setzten allerdings jahrelange Arbeit und enorme Expertise voraus. Trotzdem wird es für die Autohersteller immer schwieriger, das Problem kleinzureden. Miller und Valasek wollen ihr genaues Vorgehen nun veröffentlichen, damit andere Forscher es nachvollziehen können. „Hört auf zu erzählen, dass eure Geräte nicht hackbar sind“, sagte Valasek in Richtung der Autohersteller. „Ihr macht euch lächerlich.“

GREGOR HONSEL

Platzieren Sie Ihre Anzeige
im **meist verkauften Magazin**
im Bereich der erneuerbaren Energien

neue energie

19 603 Exemplare

energy 2.0

3 615 Exemplare

Sonne Wind & Wärme

3 283 Exemplare

Photovoltaik

2 278 Exemplare

Erneuerbare Energien

2 163 Exemplare

Kontakt:
eMedia GmbH
Christian Engelking
Tel.: +49 (0)511 5352-834
Julian Wagner
Tel.: +49 (0)511 5352-835
E-Mail: neueenergie@emedia.de

Quelle: IVW, I/2015

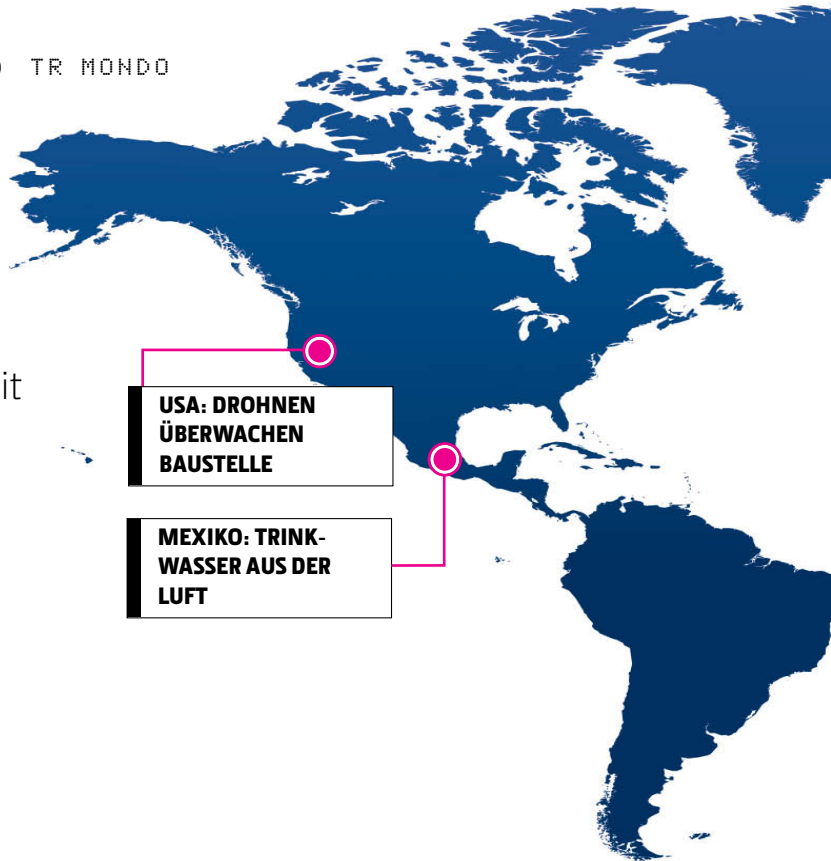
neue energie
das magazin für erneuerbare energien

Auch erhältlich im gut sortierten Bahnhofsbuchhandel.



tr mondo

Technology Review ist mit Autoren weltweit vertreten. Auf den folgenden Seiten berichten sie über die spannendsten Entwicklungen in ihren Ländern.



**USA: DROHNEN
ÜBERWACHEN
BAUSTELLE**

**MEXIKO: TRINK-
WASSER AUS DER
LUFT**

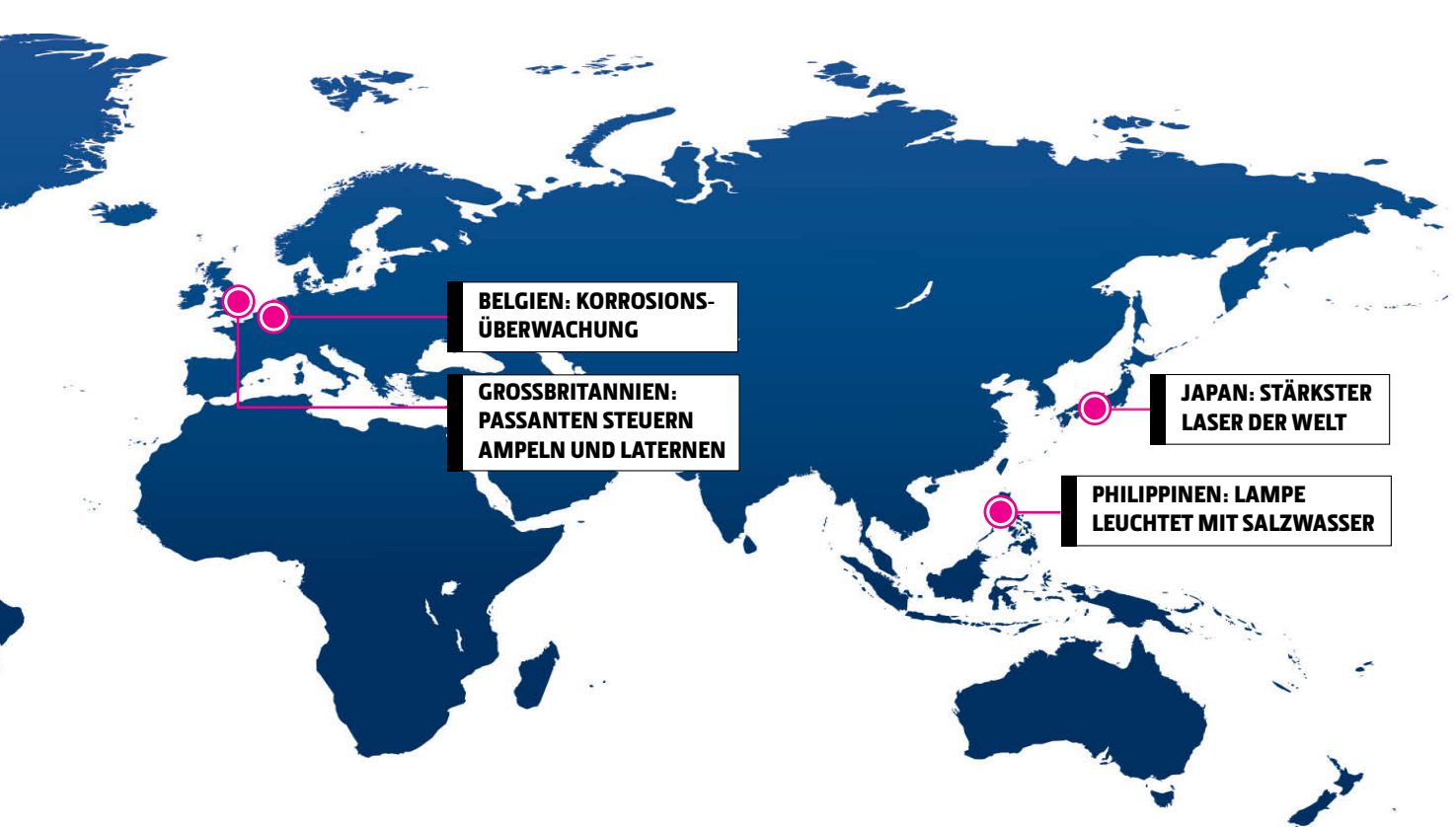


Drohnen überwachen Stadionbaustelle

Eine Software vergleicht den tatsächlichen Baufortschritt auf den Bildern der Drohnenkameras mit den dreidimensionalen Bauplänen des Stadions in Sacramento.



Fotos: University of Illinois at Urbana-Champaign



Für die Bauarbeiter eines neuen Stadions in Sacramento im US-Bundesstaat Kalifornien könnte es demnächst sehr schwierig werden, sich heimlich mal ein Päuschen zu gönnen. Ihre Baustelle überwachen Drohnen.

Einmal pro Tag überfliegen sie autonom den Neubau für die Basketballmannschaft Sacramento Kings und filmen dabei. Die Aufnahmen werden anschließend in ein dreidimensionales Bild konvertiert und von einer Software mit den digitalen Bauplänen des Stadions und der Zeitplanung für die einzelnen Abschnitte verglichen. Das Programm zeigt an, wie das Projekt vorankommt, und markiert Bereiche, die hinter dem Zeitplan liegen – und zwar fast in Echtzeit.

„Wir heben die Bereiche einer Baustelle hervor, die problematisch werden könnten“, sagt Mani Golparvar-Fard, Assistenzprofessor für Bauingenieurwesen an der Universität von Illinois, der die Software zusammen mit Kollegen entwickelt hat. „Mithilfe unserer Software können wir erkennen, warum es zu Abweichungen kommt, und wir können sehen, wo es Fortschritte bei der Effizienz gibt.“ Das Programm kann sogar anzeigen, wie unterschiedliche Subunternehmer auf der Baustelle zusammenarbeiten.

Das Projekt zeigt, wie auch körperliche Arbeit mit neuen Technologien in Zukunft kontrolliert werden könnte. Bei eher geistigen Tätigkeiten, darunter vielen Bürojobs, wird schon heute versucht, die Produktivität von Mitarbeitern mit Software auf Desktop-Rechnern und Smartphones genauer zu erfassen.

Dennoch sieht Golparvar-Fard in der Erfassung des Baufortschritts durch Drohnen keine neue Qualität der Überwachung. „Es ist nichts Neues in der Baubranche, dass etwa Vorarbeiter die Arbeiten überwachen oder feste Kameras installiert sind“, sagt er. „Natürlich fühlt es sich für die Arbeiter anders an, wenn die Kontrollen automatisch erfolgen. Aber man muss bedenken, dass es letztlich nicht um die Produktivität der Arbeiter selbst geht, sondern darum, was sie brauchen, um effizienter zu sein.“

Besonders in puncto Effizienz gibt es im Bauwesen große Defizite. Laut einem Bericht des National Research Council der USA aus dem Jahr 2009 hinkt die Bauindustrie bei der Produktivität anderen Branchen hinterher. Als Gründe dafür werden Probleme bei Planung, Koordination und Kommunikation genannt. Kein Wunder: Den Baufortschritt einer großen und komplexen

Baustelle in Echtzeit zu erfassen, ist kein leichtes Unterfangen.

Zwar sei es bereits heute üblich, den Baufortschritt genau im Auge zu behalten, betont Lincoln Wood von Turner Construction, Generalunternehmer des Stadionneubaus. Die Analysen von Golparvar-Fard könnten jedoch erkennen lassen, wie sich Verzögerungen in einem Bereich auf das ganze Projekt auswirken, sagt der Regionsmanager für virtuelles Design und Bau. „Das Schöne daran ist, dass alle Arbeiten in einem Gebiet gezeigt werden, sodass man einen Blick auf den Gesamteffekt bekommt.“

Doch Golparvar-Fard möchte noch mehr Details – und das in Echtzeit. Sein Team testet derzeit ein System, bei dem Drohnen Kameras flächendeckend auf Baustellen installieren, die so kontinuierlich überwacht werden. Darüber hinaus experimentieren sie mit einer Crowdsourcing-Plattform zur Kategorisierung der verschiedenen Tätigkeiten im Videomaterial. Ein Manager könnte sehen, wie unterschiedliche Aufgaben insgesamt erledigt werden und wie viel Zeit verschiedene Bauarbeiter dafür benötigen.

WILL KNIGHT



Yves Van Ingelgem
hat ein neues
Verfahren zur
Korrosionserken-
nung entwickelt.



An dem ersten deutschen
Offshore-Windpark
Alpha Ventus nagt schon
der Rost. Van Ingelgem
könnte sagen, wie tief.

Foto: Matthias Ibeler/ Alpha Ventus

BELGIEN

Rost-Erkennung in Echtzeit

Offshore-Windenergieanlagen sind täglich nicht nur Wind und Wetter ausgesetzt. Bis zu vierzig Meter hohe Stahlfundamente müssen unter Wasser Strömung und Salzwasser standhalten und die bis zu 140 Meter hohen Türme und Rotoren tragen. Dabei nagt der Rost andauernd an der Konstruktion. Die Frage ist nur, wie schnell.

Der 33-jährige Belgier Yves Van Ingelgem hat jetzt eine Technik entwickelt, die eine kontinuierliche Materialprüfung solcher Fundamente in Echtzeit ermöglicht. Der Schlüssel des Verfahrens ist ein Algorithmus zur Materialkorrosion, den Van Ingelgem während seiner Zeit als Doktorand an der Freien Universität in Brüssel entwickelt hat.

Um die Korrosion zu messen, werden an den Fundamenten der Windenergieanlagen Sensoren angebracht. „Wir messen aber nicht den tatsächlichen Materialschwund, sondern die Aktivität des Korrosionsvorgangs selbst“, erklärt Van Ingelgem. Außerdem verspricht er, auch Materialermüdungen und

Verformungen ausmachen zu können. Liefern will er „ein integrales Bild des Gesundheitszustandes der Struktur“.

Die Sensoren an den Fundamenten bestehen aus einer Elektrode im Inneren der Struktur und einer zweiten außen auf der Oberfläche. Anschließend fließt ein Multifrequenz-Wechselstrom zwischen beiden Elektroden. Der resultierende Stromverlauf wird aufgezeichnet und von Van Ingelgems Algorithmus ausgewertet. So lässt sich bereits in einem sehr frühen Stadium sagen, ob und wo die Fundamente rosten, sich verformen oder sonstige Schäden aufweisen. „Wir bringen die Sensoren dort an, wo wir aus Erfahrung wissen, dass das Material leidet“, erklärt Van Ingelgem. Das ist vor allem unter der Wasseroberfläche, an Schweißnähten und am Meeresboden der Fall.

Um die Technologie zu vermarkten, gründete Van Ingelgem das Unternehmen Zensor. Derzeit läuft ein Feldversuch in zwei Windparks. In einem dritten soll die Technologie demnächst installiert werden. Der junge Unternehmensgründer hat nach eigenen Angaben

weitere Kunden auf der Warteliste. Die Kosten für ein „basic setup“ belaufen sich auf rund 5000 Euro.

Für die Betreiber von Windparks lohnt sich die neue Messtechnik, denn sie ermöglicht frühzeitige Instandhaltungsarbeiten an den richtigen Stellen. Die Lebensdauer der Strukturen verlängert sich, die Ausgaben für Reparaturen, das Unfallrisiko und damit auch die Versicherungsprämien sinken.

Van Ingelgems Technologie könnte allerdings nicht nur bei den Fundamenten der Windgeneratoren gute Dienste leisten. Auch die Transformatorstationen auf hoher See sind korrosionsanfällig. Außerdem seien seine Sensoren noch für andere große Infrastrukturbauten nützlich, erklärt der Ingenieur. Auch zum Beispiel Brücken, Pipelines oder Industrieanlagen enthalten viele Stahlteile und rosten. Das geht bis hin zu den unterirdischen Tanks ganz normaler Tankstellen.

REINER WANDLER

Maker Faire® Berlin

FAMILIEN-FESTIVAL FÜR INSPIRATION,
KREATIVITÄT & INNOVATION

DER GROSSE MAKER-TREFFPUNKT.



3. & 4. Oktober 2015
Postbahnhof Berlin

präsentiert von:

Make:
make-magazin.de

Goldschmied:



Silberschmied:



Kupferschmied:



Kooperationspartner:



Medienpartner:



Berliner Woche



NEUKÖLLNER-NET



Tickets und weitere Informationen unter

WWW.MAKERFAIRE.BERLIN



🇬🇧 GROSSBRITANNIEN

Ross Atkin und die wartende Ampel

„**Einen Großteil meiner Zeit** verbringe ich damit, Menschen mit Behinderungen hinterherzulaufen“, sagt der Londoner Designer Ross Atkin. Er will wissen, welche Hindernisse eine Stadt für sie bereithält – um sie dann zu beseitigen. Dabei sind Atkin eine Reihe von Ideen gekommen. Straßenlaternen etwa, die für ältere Menschen heller leuchten, oder Lautsprecher, die Blinden verraten, welches der sieben nebeneinanderliegenden Geschäfte der meistgesuchte Supermarkt ist, oder eine interaktive Straßenkarte, die ausländischen Besuchern in der jeweiligen Muttersprache den Weg ins Museum weist. Zusammen mit Marshalls, einer Firma für Stadtgestaltung, will er Ideen wie diese nun umsetzen. Bis Ende des Jahres sollen sprechende Demosäulen aufgestellt und eine App entwickelt werden. Atkin und seine Partner hoffen anschließend auf größeres Interesse auch aus anderen Gemeinden.

Steuerbare

Außenanlagen können aber auch Ampeln sein, die so programmiert sind, dass sie für angemeldete Passanten länger grün bleiben. Das Ampelprojekt ist Atkin am wichtigsten, „vier von fünf Menschen über 65 Jahren kommen nicht rechtzeitig über die Straße“, sagt er. Doch gerade die individuelle Anpassung von Ampelphasen ist in der Umsetzung am schwierigsten. Denn viele Verkehrsampeln sind mit umliegenden Ampeln in einem Takt geschaltet. Abweichungen davon würden den gesamten Verkehrsfluss beeinträchtigen.

Angefangen hat alles mit einem Forschungsprojekt zur Inklusion im Straßenverkehr. So wurde er auf Menschen aufmerksam, die mit Einschränkungen am Straßenverkehr teilnehmen. Dabei erkannte er, dass fest installierte Hilfsmittel dem einen nutzen, aber dem anderen schaden können. Für einen Blinden etwa sind taktile Wegweiser auf dem Fußweg eine große Hilfe, für einen Menschen im Rollstuhl sind diese Unebenheiten dagegen eher störend. So kam Atkin auf die Idee der steuerbaren Außenanlagen.

Übernommen hat Atkin sie von „Responsive Websites“, die sich an die Bedürfnisse des Nutzers anpassen – je nachdem, ob man eine Homepage mit dem Handy, Tablet oder PC öffnet. „Im Straßenverkehr gilt nicht, dass eine Lösung allen hilft, daher kam ich auf die Idee, die Funktionsweise von Responsive Websites auf die Straße zu übertragen“, sagt Atkin.

Schon bald sollen sich Hilfsbedürftige bei Atkins Dienst anmelden können und eingeben, welche Art von Hilfe sie benötigen. Diese Informationen werden anschließend an einen Bluetooth-Anhänger von der Größe einer Zwei-Euro-Münze gesendet. Der Anhänger soll sechs Pfund kosten (acht Euro) und mit einer Batterie ein Jahr lang laufen. Kommen Nutzer mit dem Anhänger in der Tasche an einer steuerbaren Anlage vorbei, reagieren die Geräte automatisch entsprechend der Bedürfnisse der Nutzer. „Das macht das Erleben viel natürlicher“, sagt der Designer.

INES NASTALI



Mit dem Bluetooth-Anhänger von Ross Atkin in der Tasche wird die Straßenlaterne beim Vorbeigehen heller, und der Stadtplan fängt an zu sprechen.



JAPAN

Stärkster Laser der Welt

Der Schuss dauerte zwar nur das Billionstel einer Sekunde, pulverisierte aber alle Rekorde. Im Sommer feuerten Forscher an der japanischen Universität Osaka den stärksten Laser der Welt ab. Für einen winzigen Augenblick lag seine Leistung bei zwei Billionen Watt oder zwei Petawatt. Sie war damit doppelt so hoch wie die des zweitstärksten Lasers der Welt, der gerade an der Universität Texas in Austin entwickelt wird.

Mit ihrem Rekord verleiteten die japanischen Forscher viele Medien sofort zu Vergleichen mit Science-Fiction, wie etwa der Laserkanone des Todessterns aus dem Weltraumabenteuer „Star Wars“, die mit einem Schuss einen ganzen Planeten zerstören kann. Abgesehen davon, dass die Leistung des LFEX (Laser for Fast Ignition Experiments) dafür bei Weitem nicht ausreicht, sind die von den Japanern angedachten Anwendungsgebiete sehr friedlicher Natur.

Denn der Forschungslaser in Osaka hat die Fähigkeit, starke Quantenstrahlen, also energiereiche Röntgen- und Gammastrahlen, zu erzeugen. Sie könnten mittelfristig sowohl in der Strahlentherapie von Krebspatienten als auch in der Materialprüfung etwa von Brückenbauwerken eingesetzt werden. Vor allem aber halten die Forscher mit dem 100 Meter langen LFEX einen Durchbruch in der Kernfusion für möglich, bei der die Verschmelzung von Deuterium und Tritium durch energiereiche Licht- oder Teilchenstrahlen ausgelöst wird.

Trotz des Weltrekords geht die Entwicklung des Lasers weiter. „Unser Ziel ist es nun, die Leistung auf zehn Petawatt zu erhöhen“, erklärte Professor Junji Kawanaka.

MARTIN KOELLING



Der LFEX (Laser for Fast Ignition Experiments) an der Universität von Osaka ist der stärkste Laser der Welt.

Foto: Institute of Laser Engineering / Osaka University



In vielen Ländern mit Wassermangel herrscht eine hohe Luftfeuchtigkeit. Daraus will Edgar Rodríguez Trinkwasser gewinnen.

Foto: Fotolia



MEXIKO

Trinkwasser aus der Luft

In vielen Regionen Lateinamerikas beträgt die Luftfeuchtigkeit bis zu 100 Prozent. Das brachte Edgar Rodríguez auf eine Idee: Warum nicht daraus Trinkwasser gewinnen? Das wertvolle Gut wird weltweit knapp. Laut Studien der Vereinten Nationen (UNO) werden im Jahr 2025 zwei Drittel der Erdbbevölkerung unter Wasserknappheit leiden. 1,8 Milliarden Menschen haben dann schätzungsweise überhaupt keinen Zugang zu sauberem Trinkwasser mehr.

Rodríguez, ein 30-jähriger Ingenieur an der Universidad Nacional Autónoma in Mexiko, will das nicht akzeptieren. Er arbeitet an einem Kondensator, auch Kondensor genannt, der aus Luftfeuchtigkeit mittels Sonnenenergie Trinkwasser gewinnt. In einem schwarzen Kamin werden dazu mehrere feinmaschige Filter installiert. Scheint die Sonne auf die schwarze Oberfläche des Kamins, heizt sich die Luft darin auf. Die warme und feuchte Luft steigt auf und strömt zuerst durch einen Reinigungsfilter, bevor sich die Feuchtigkeit als Tropfen an immer feinmaschigeren Netzen oben im Kamin niederschlägt. Das entstandene Wasser wird anschließend aufgefangen. Bei Sonnenschein und hoher Luftfeuchtigkeit kommen dabei bis zu 100 Liter pro Tag zusammen.

Die Gewinnung von Luftfeuchtigkeit als Trinkwasser an sich ist nicht neu. „Sie wurde bereits in Ländern wie Peru erprobt“, erklärt Rodríguez. Dort stehen die Anlagen an sehr windigen Orten hoch in den Anden. Denn eine hohe und gleichförmige Luftströmung ist Voraussetzung für diese Art der Kondensation. Bei anderen Systemen wird die Luft für die Kondensation oft gekühlt. Das geschieht häufig mit Kompressoren, die viel Energie verbrauchen und daher nicht besonders effizient sind. Rodríguez' Technologie dagegen arbeitet völlig autark. Sie kann überall eingesetzt werden, wo die Sonne scheint, und verbraucht keine zusätzliche elektrische Energie.

MAXIMILIANO CORREDOR



Mit einer Tasse
Salzwasser leuchtet
die SALT-Lampe rund
acht Stunden lang.

PHILIPPINEN Leuchtkraft aus Meerwasser

Foto: SALT

Die Philippin Aisa Mijeno hat eine Lampe erfunden, die ihren Strom aus einfachem Salzwasser gewinnt. Die Idee kam der Lehrerin an der Universität in Lipa, als sie im Rahmen ihrer Mitarbeit bei Greenpeace bei einer der 16 Millionen philippinischen Familien lebte, die keinen Zugang zur Stromversorgung haben. Die meisten der 7000 philippinischen Inseln hängen bis heute nicht am Netz. „Die Menschen mussten zwölf Stunden gehen, um in der 50 Kilometer entfernten Stadt Kerosin für ihre Lampen zu kaufen“, berichtet Mijeno. Außerdem ist Kerosin leicht entflammbar und sorgt dadurch immer wieder für Unfälle, und die Abgase verpesten die Atemluft in den Wohnungen.

„Wir erinnern uns alle an die Zitrone mit zwei Elektroden als Batterie im Unterricht“, erklärt Mijeno das Grundprinzip ihrer Lampe. Sie funktioniert wie eine einfache galvanische Zelle. Zwei Elektroden, eine Anode und eine Kathode, werden in eine Elektrolytlösung – in diesem Falle Wasser mit Kochsalz – getaucht. Die Elektronen beginnen, von der negativ geladenen Anode zur positiven Kathode zu wandern. Dabei fließt Strom.

„Sustainable Alternative Lightning (SALT)“ heißen sowohl das Projekt als auch das Unternehmen, das Mijeno zusammen

mit ihrem Bruder Raphael ins Leben gerufen hat. Mit einem Glas Wasser und zwei Esslöffeln Salz liefert SALT genug Energie, um eine LED mit 90 Lumen acht Stunden lang leuchten zu lassen. Das entspricht in etwa einer Lichtstärke von acht Kerzen. Wer an der Küste lebt, kann auch einfach Meerwasser in die Lampe kippen. Der durchschnittliche Salzgehalt der Ozeane ist für den Betrieb ausreichend.

Die nächste Version von SALT soll eine Lichtstärke von 350 Lumen erreichen und eine Lademöglichkeit für Smartphones über einen USB-Anschluss bieten. Außerdem soll die ganze Lampe wasser- und stoßfest werden, um die Lebensdauer zu erhöhen. Die Elektroden halten je nach Gebrauch bis zu einem Jahr, dann müssen sie ausgetauscht werden. Die LEDs haben bei guter Behandlung eine Lebensdauer von über zehn Jahren.

Die Lampe wird spätestens Anfang kommenden Jahres zu kaufen sein und um die 35 Dollar kosten. Diesen Preis hoffen die jungen Unternehmer durch entsprechend hohe Stückzahlen noch drücken zu können.

REINER WANDLER
WWW.SALT.PH



impressum

Technology Review ist die deutsche Lizenzausgabe der MIT Technology Review

REDAKTION

Postfach 61 04 07, 30604 Hannover, Karl-Wiechert-Allee 10,
30625 Hannover, Telefon: 0511/53 52-764,
Fax: 0511/53 52-767

www.technologyreview.de, E-Mail: office@tr.heise.de

CHEFREDAKTEUR: Robert Thielicke

REDAKTEURE/-INNEN: Gregor Honsel, Jennifer Lepies
(Online), Karsten Schäfer, Dr. Wolfgang Stieler, Veronika
Szentpétery

REDAKTIONSASSISTENZ: Stephan Brünig

SCHLUSSREDAKTION: Timo Ahrens

LAYOUT: Frank Heymann, Andreas Zickert

BILDBEARBEITUNG: Eric Tscherne

INFOGRAFIKEN: Brian Sipple

FOTOREDAKTION: Heike Pankel

MITARBEITER DIESER AUSGABE: Maximiliano Corredor,
Astrid Dähn, Dr. Uta Deffke, Udo Flohr, Ulf J. Froitzheim,
Daniel Hautmann, Dr. Christian Honey, Peter Ilg, Will Knight,
Martin Koelling, Jan Oliver Löffken, Sascha Mattke, Bernd Mül-
ler, Ines Nastali, Antonio Regalado, Amanda Schaffer, Joseph
Schepbach, Ben Schwan, Tom Simonite, Tobias Stolzenberg,
Talbot, Reiner Wandler, Eva Wolfangel, Elena Zafra

VERLAG

Heise Medien GmbH & Co. KG, Postfach 61 04 07, 30604
Hannover, Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 0511/53 52-0, Fax: 0511/53 52-129

HERAUSGEBER: Christian Heise, Ansgar Heise

GESCHÄFTSFÜHRER: Ansgar Heise, Dr. Alfons Schröder

VERLAGSLEITER: Dr. Alfons Schröder

ANZEIGENLEITUNG: Michael Hanke,

Telefon: 0511/53 52-167, Fax 0511/53 52-200,

michael.hanke@heise.de, www.heise.de/mediadaten/tr

ANZEIGENPREISE: Es gilt die Preisliste vom 1. Januar 2015

LEITER VERTRIEB UND MARKETING: André Lux

VERTRIEBSABTEILUNG: 0511/53 52-157 (Aboservice:
040/3007-3525), Vertrieb Einzelverkauf: VU Verlagsunion KG,
Am Klingenweg 10, 65396 Walluf; Tel.: 06123/620-132,
Fax: 06123/620-5132;

E-Mail: info@verlagsunion.de, Internet: www.verlagsunion.de

SONDERDRUCK-SERVICE: Julia Conrades

DRUCK: Dierichs Druck + Media GmbH & Co. KG, Frankfurter
Str. 168, D-34121 Kassel, ISSN 1613-0138

ABOSERVICE

Heise Medien GmbH & Co. KG, Leserservice,
Postfach 24 69, 49014 Osnabrück
Telefon: 0541/800 09-120, Fax: 0541/800 09-122,
E-Mail: leserservice@heise.de, Internet: www.heise.de/abo

ABONNEMENT-PREISE

Standardabo inkl. Versandkosten im Inland € 114,60, in
Österreich € 118,80, in Europa € 120,00, im restl. Ausland
(außer Schweiz) € 120,60 (CHF 139,20); ermäßigtes Abo für
Auszubildende, Schüler, Studenten, Zivil- und Grundwehr-
dienstleistende (nur gegen Vorlage einer entsprechenden
Bescheinigung) inkl. Versandkosten € 75,00, in Österreich
€ 76,80, in Europa € 78,00, im restl. Ausland (außer Schweiz)
€ 78,60 (CHF 90,00). Das Technology-Review-plus-Abo
kostet pro Jahr € 4,80 (CHF 12,00) Aufpreis.
Der Bezug der Zeitschrift Technology Review ist im Mitglieds-
beitrag des Verbandes ADT, des hightech presseclub e.V. und
des Vereins Munich Network e.V. enthalten. Für VDI-, VBIO-,
VDE-, GI- (Gesellschaft für Informatik), bdvb e.V., /ch/open
und JUG Switzerland-Mitglieder gilt ein ermäßigter Preis im
Inland von € 88,20, in Österreich € 95,40, in Europa € 95,40,
im restl. Ausland (außer Schweiz) € 96,00 (CHF 110,40) gegen
Vorlage eines schriftlichen Nachweises des Verbandes bzw.
Vereins einmal pro Jahr. Eine Haftung für die Richtigkeit der
Veröffentlichungen kann trotz sorgfältiger Prüfung durch
die Redaktion vom Herausgeber nicht übernommen werden.
Kein Teil dieser Publikation darf ohne ausdrückliche schrift-
liche Genehmigung des Verlags in irgendeiner Form repro-
duziert oder unter Verwendung elektronischer Systeme ver-
arbeitet werden. Für unverlangt eingesandte Manuskripte
kann keine Haftung übernommen werden.

PRINTED IN GERMANY, COPYRIGHT 2015 BY HEISE
MEDIEN GMBH & CO. KG

institutionen

Adobe	67 f.
Alcoa	73, 74
Allen Institute for	
Artificial Intelligence	45
Apple	43, 53 f., 67, 86
AT&T	43
ATI	73, 74
Atlantic	85
Baidu	43
Bayerischer Verfassungsgerichtshof	69
Bell Labs	43
Bild	69
BMW	56
BSI	69
BTC	83
Bundestag	67, 82
BVL	50
Carnegie Mellon University	76, 79
Center for Automotive	
Embedded Systems Security	56
CNBC	86
Compaq	85
Cylab	73
Die Welt	69
Dropbox	70
Ebay	67, 85
EZB	67
Facebook	42 ff., 70
FBI	72, 76
Fiat Chrysler	54
Forbes	56
Ford	54 f.
Fortune	85
Fraunhofer-Institut für sichere	
Informationstechnik	82
GCHQ	69
General Motors	54
Google	43 f., 53 f., 70
Hacking Team	68
Hewlett-Packard	54
IBM	43
JP Morgan	67
Kings College London	70
Los Angeles Times	86
Ludwig-Maximilians-Uni München	79
McAfee	67
Massachusetts Institute of Technology	69
Mercedes	56, 70
Microsoft	43, 69
Monsanto	50
Motorola	54, 56
Nasa	86
NASDAQ	67
National Safety Council	53
National Science Foundation	86
New York University	43 f.
Nexus	53
NSA	69 f.
Nvidia	53
Opel	56
ORF	56
PayPal	85
Risk Based Security	67
RSA Security	68
Saudi Aramco	67 ff.
Security Research Labs	82
Siemens	70
Skype	54
Solarworld	73, 76
Sony	67
SpaceX	85, 86
Spiegel	69
Stanford University	55
Starbucks	53
Tesla	55, 85 f.
Time	85
Toyota	54 f.
Uni Bonn	79, 80
Uni Passau	69
United Steelworkers	73, 74, 76
Universität Penn State	74
Universität Stuttgart	79
Universität von Arkansas	50

IMMER EINE IDEE SCHLAUER.



2x Mac & i mit 30% Rabatt testen!

Ihre Vorteile:

- **Plus:** digital und bequem per App
- **Plus:** Online-Zugriff auf das Artikel-Archiv*
- **Lieferung frei Haus**

Für nur
13,80 €
statt 19,80 €

Jetzt bestellen und von den
Vorteilen profitieren:

**mac-and-i.de/
miniabo**

0541 80 009 120
leserservice@heise.de

* Für die Laufzeit
des Angebotes.



Mac & i.
Deutlich. Mehr. Wissen.

fokus

IT-Sicherheit



66	TREND
70	INTERVIEW
72	SPIONAGE
78	BEDIENBARKEIT
82	LEGALITÄT

Ob Bundestag oder IT-Anbieter – niemand ist mehr vor Datendiebstahl gefeit
 Webfahnder Thomas Rid über den besten Weg, Übeltäter im Netz zu entlarven
 Die USA erheben erstmals Klage gegen Online-Spione
 Sicherheit und Anwenderfreundlichkeit müssen keine Gegensätze sein
 Hacker im Dienst des Cyber-Schutzes arbeiten in einer gesetzlichen Grauzone

Zeitalter der Massenhacks

Die Zahl **riesiger Datendiebstähle nimmt zu**, selbst etablierte IT-Unternehmen scheinen den Angriffen der Hacker schutzlos ausgeliefert zu sein. Ist der Kampf verloren?
 VON CHRISTIAN HONEY

Es ist der 15. August 2012. Die meisten Mitarbeiter feiern bei ihren Familien den Ramadan, als die Computer der Ölfirma Saudi Aramco zu spinnen beginnen: Bildschirme flickern, manche Rechner reagieren gar nicht oder schalten sich von selbst ab. Dann verschwinden Dateien, ganze Festplatten sind plötzlich gelöscht, das interne Netzwerk bricht vollständig zusammen. Noch bevor die Handvoll anwesender Mitarbeiter versteht, was gerade geschieht, sind mehr als 30.000 Rechner unbrauchbar oder ein großer Teil ihrer Daten ist unwiederbringlich gelöscht.

Die Firma Risk Based Security spricht in ihrem Jahresbericht von weltweit 3014 Fällen von Datenverlust allein im vorigen Jahr. Dabei sollen insgesamt 1,1 Milliarden Datensätze erbeutet worden sein. Für denselben Zeitraum nennt der Verizon Data Breach Investigations Report 2122 bestätigte Fälle. Einig sind sich die Quellen darin, dass mindestens 80 Prozent der Diebstähle auf das Konto von Hackern gehen. Den Gesamtschaden durch Hackerangriffe im Jahr 2014 schätzt der IT-Sicherheitsspezialist McAfee auf 375 Milliarden US-Dollar.

Unter den Opfern großer Hacks sind immer wieder auch Institutionen, für die Datensicherheit ein wesentlicher Teil der täglichen Arbeit sein sollte. Seit 2010 waren unter den Betroffenen Finanzinstitute (NASDAQ, JP Morgan), globale Technologieunternehmen (Apple, Ebay, Adobe, Sony), Behörden (die EZB, US Office of Personnel Management) und ein Parlament (der deutsche Bundestag).

Wie kommt es, dass sich selbst milliarden-schwere Konzerne, etablierte IT-Firmen und staatliche Institutionen gegen Hacker-Angriffe offenbar



kaum wehren können? Ist die Sicherheitstechnologie nicht ausgereift genug? Fehlt es den Nutzern an Expertise? Oder macht die Architektur von Rechnern und IT-Netzen Hacks schlicht unvermeidbar?

Um Zugriff auf einen Rechner oder ein Netzwerk zu erlangen, gibt es unterschiedliche Wege. Einer davon besteht darin, über das Internet nach Schwachstellen, sogenannten Remote Exploits, zu suchen. Dazu braucht ein Hacker lediglich eine IP-Adresse: Mit ihr kann er einen entfernten Rechner nach offenen Ports durchsuchen, zum Beispiel jenen Schnittstellen, über die E-Mail- und Chat-Programme oder Internet-Browser mit dem Internet verbunden sind. Oft verrät ein solcher Port-Scan viel über die Architektur und die Sicherheitsvorkehrungen des Computers, etwa welche Programme seine Ports nutzen und welches Betriebssystem auf dem Rechner läuft. Für Hacker gibt es heute sogar kostenlose Software wie „Metasploit“, mit der selbst Unerfahrene ohne viel Programmierkenntnis einen fremden Rechner nach Schwachstellen abklopfen können.

Mit den so gewonnenen Informationen kann sich ein Hacker auf die Suche nach bekannten Exploits machen. Entweder testet seine Angriffssoftware die Schwachstellen automatisch, oder er wird in Internet-Foren fündig, in denen sich Interessierte darüber austauschen, wie sie etwa an Login-Daten kommen. Sind diese ergattert, kann der Hacker eine Schadsoftware auf der Plattform ausführen und die computereigene Überwachung des Datenverkehrs oder Anti-Virus-Programme lahmlegen.

Ein anderer Weg in einen Computer führt über den ahnungslosen Nutzer am Bildschirm. Beim Ölkonzern Aramco, so stellte sich später heraus, hatte Mitte des Jahres ein Mitarbeiter auf einen unverdächtig erscheinenden Link in einer E-Mail geklickt. Hinter dem Link verbarg sich der Virus Shamoon, der unbemerkt den Rechner des Mitarbeiters infiltrierte und von dort aus das ganze Aramco-Netzwerk. Laut dem Bericht von Verizon machen solche „Phishing“-Angriffe heute 20 Prozent aller Cyber-Angriffe aus, Tendenz seit Jahren steigend.

So kann ein einziger Klick in einer E-Mail Millionenschäden anrichten: Ohne wichtige Vertragsdaten, ohne E-Mail-Adressen, ohne die gespeicherten Belieferungsstrukturen musste Saudi Aramco, das täglich rund 12,5 Millionen Tonnen Öl fördert, wochenlang auf Papierformulare zurückgreifen. Lieferungen verzögerten sich. Bald verschenkte Saudi Aramco sein Öl sogar, um Lieferlücken zu vermeiden. Das Unternehmen selbst bezifferte den Schaden auf rund 15 Millionen US-Dollar. Medienberichte sprachen von bis zu 750 Millionen Dollar.

Whitfield Diffie, Sicherheitsforscher und Erfinder des Public-Key-Verfahrens, warnt aber davor, dem einzelnen Mitarbeiter die Schuld die Schuhe zu schieben. „Beim Hack auf die Firma RSA Security von 2011 zum Beispiel hatte ein Mitarbeiter eine Excel-Tabelle in einer völlig normal anmutenden E-Mail geöffnet“, sagt Diffie. „Schnell war der Großteil des Netzwerks seines Arbeitgebers kompromittiert, und es wurden Sicherheitscodes geklaut, mit denen sich weltweit Menschen authentifizieren.“

In Fällen wie Saudi Aramco oder RSA Security hätten Mitarbeiter einfach keine Chance, hinter einer E-Mail einen Angriff zu erkennen. Das tiefer liegende Problem bestehe darin, dass es eine Schadsoftware auf Computern sehr leicht hat. Denn die Architektur der heutigen Geräte erlaubt es selbst Verwaltungssoftware wie Excel, jeden beliebigen Code auf dem Rechner auszuführen. Hat ein Angreifer also erst mal Zugang zu einem Computersystem, bekommt er über eingeschleusten Code viel zu schnell Zugriff auf alle Funktionen.

Zwar werden Schwachstellen von Software-Anbietern schnell geflickt, auf Englisch „gepatcht“. Systemadministratoren erledigen aber die neuesten Updates oft nicht zügig genug. So bleibt Hackern viel Zeit, um Systeme über ein bekanntes Exploit anzugreifen und dabei wieder neue Angriffspunkte auszumachen. Dem Sicherheitsbericht von Verizon zufolge werden Exploits in 99,9 Prozent der Fälle mehr als ein Jahr, nachdem die eigentliche Schwachstelle bekannt wird, zum ersten Mal ausgenutzt. Im Jahr 2014 sollen 97 Prozent aller Exploits auf nur zehn bereits bekannte Sicherheitsmängel zurückführbar gewesen sein.

Schafft ein Hacker es, eine bisher unbekannte Schwachstelle, ein sogenanntes Zero-Day-Exploit, aufzuspüren, hängt es von seinem Charakter ab, ob er damit nur seine Ehre mehrt oder auch sein Einkommen (siehe Seite 82). Während der letzten Jahre hat sich ein blühender weltweiter Markt für Zero-Day-Exploits entwickelt. Auf Darknet-Portalen verkaufen Hacker sie wie in einem normalen Online-Shop – an Hackerkollegen, an Unternehmen oder staatliche Institutionen und sogar an ihre Opfer. „TheRealDeal Market“ etwa ist nur über die Anonymisierungs-Software TOR erreichbar. Statt illegaler Drogen werden hier „Code-Raritäten“ feilgeboten, wie es auf der Seite heißt.

Zum Beispiel verkaufte ein Hacker namens Tovi der italienischen Cybersecurity-Firma Hacking Team im Oktober 2013 ein Zero-Day-Exploit des Adobe Flash Players zum Preis von 45 000 US-Dollar, anstatt Adobe auf die Schwachstelle aufmerksam zu machen. Ironischerweise flog der Handel auf – nach einem Hack gegen Hacking Team selbst: Im Oktober 2014 waren rund 400 Gigabyte firmeninterner Daten von Hacking Team mithilfe des Filesharing-Protokolls Bittorrent veröffentlicht worden, inklusive der Rechnungen und E-Mails, aus denen hervorging, dass Hacking Team Zero-Day-Exploits kauft und weltweit Unternehmen und Regierungen anbietet.

Just in diese Gemengelage platzen Regierungen nun mit einem Vorhaben, das die Sicherheit im Netz weiter schwächen dürfte – falls es umgesetzt wird. Vordergründig geht es nur um verschlüs-

selte Kommunikation: Aus Sorge vor der wachsenden Terroris-
musgefahr fordern Nachrichtendienste wie der britische GCHQ
und die amerikanische NSA einen Sonderzugang, um alle ver-
schlüsselte Kommunikation mitlesen zu können. Englands Pre-
mierminister David Cameron kündigte bereits für den Herbst die-
ses Jahres an, entsprechende Gesetze erarbeiten zu lassen. Konkret
soll alle verschlüsselte Kommunikation samt der Schlüssel gespei-
chert werden und mit einer Art Generalschlüssel, der nur mit
richterlichem Beschluss zugänglich ist, entschlüsselbar bleiben.

In Wahrheit würde die Maßnahme jedoch viel weitere
Kreise ziehen. Denn die Softwareschlüssel dienen auch zur
Authentifizierung: Nur über sie weiß etwa ein Microsoft-Pro-
gramm, dass ein Update wirklich von Microsoft stammt – und
keine Schadsoftware ist. Kämen sie in die Hände von Hackern,
stünde ihnen Tür und Tor offen. Viele IT-Sicherheitsexperten
halten Camerons Vorschläge daher für Unsinn. In einem ge-
meinsam verfassten Artikel warnten im Juni 15 US-Professoren
davor, sich von den bewährten Verfahren der IT-Sicherheit
abzuwenden. Dazu gehöre vor allem das Prinzip der Vorwärts-
sicherheit, also einmal verwendete Schlüssel nicht zu speichern,
sondern nach dem Ver- und Entschlüsseln sofort zu löschen.
„Das Prinzip stellt sicher, dass ein Angreifer keine Schlüssel mehr
auf einem Rechner finden kann, die in der Vergangenheit genutzt
wurden“, sagt Ronald Rivest, Mitautor des Artikels und Professor
für Elektrotechnik und Informatik am Massachusetts Institute
of Technology. „Vorwärtssicherheit bedeutet damit, dass keine
Nachrichten aus der Vergangenheit mehr entschlüsselbar sind,
selbst wenn jemand sie auf ihrem Weg abfängt und kopiert.“

Ein behördlicher Sonderzugriff auf verschlüsselte Kommu-
nikation verlange nach einer extrem aufwendigen globalen Ver-
waltung der Schlüssel mit Tausenden von Mitarbeitern. „So
etwas würde auch die Gefahr von Insider-Angriffen erhöhen“,
gibt Rivest zu bedenken. Je komplexer ein System, desto schwä-
cher sei seine Sicherheit. „Und desto wahrscheinlicher treten
neue unbekannte Schwachstellen und Exploits auf.“

Rivest und Diffie sind sich einig, dass ein Sonderzugang zu
verschlüsselter Kommunikation bestenfalls „dumme Kriminelle“
überführen kann. Denn per sogenannter Peer-to-Peer-Kommu-

nikation könnten die Täter einen dazwischengeschalteten Ser-
vice-Provider einfach umgehen. Für halbwegs versierte Böse-
wichte ist das kein Problem. Auch aus rechtlicher Perspektive
scheint ein Verschlüsselungsverbot fragwürdig (siehe Kasten).

Obendrein sind auch staatliche Institutionen nicht datensicher.
Das haben nicht nur die Snowden-Enthüllungen gezeigt, sondern
auch der Angriff auf das interne Netzwerk des deutschen Bundes-
tags ParlaKom: Anfang Mai berichtete „Spiegel Online“ von ei-
ner mehrere Tage währenden Attacke. Rund einen Monat später
schrieb „Die Welt“ unter Berufung auf Sicherheitskreise, dass sich
eine Schadsoftware auf einem Rechner installiert habe, als ein
Parlamentsmitarbeiter einen Link in einer E-Mail angeklickt hatte.
Erst als fast alle 20 000 Rechner des Netzwerks befallen waren und
interne Daten nach außen versandt hatten, fiel der Angriff auf.

Anders als beim Ölkonzern Saudi Aramco waren für die
Überwachung des Bundestags-Netzwerks allerdings nicht eine
Handvoll IT-Mitarbeiter während des Ramadans zuständig, son-
dern die Experten des Bundesamtes für Sicherheit in der Infor-
mationstechnik (BSI). Aus vertraulichen Dokumenten, die eine
Quelle im Bundestag an die „Bild“-Zeitung geschickt hatte, wur-
de deutlich, dass der Abfluss von Daten dem BSI selbst gar nicht
aufgefallen war. Erst ein ausländisches Unternehmen, das für
eine befreundete Regierung arbeitet, machte das BSI darauf auf-
merksam, dass ParlaKom womöglich gerade angegriffen wurde.

Thomas Rid vom University College London betont, dass es
besonders bei den deutschen Sicherheitsbehörden extremen
Nachholbedarf gebe (siehe Seite 70). Mit gerade mal 15 ausrei-
chend qualifizierten und erfahrenen Mitarbeitern sei das BSI
personell hoffnungslos unterbesetzt. Eigene Expertise fehle weit-
gehend. Deshalb seien deutsche Behörden heute von ausländi-
schen Firmen und Sicherheitsdiensten abhängig.

Solange also Unternehmen und Behörden die Experten feh-
len und sie ihre Mitarbeiter nicht besser schulen, solange be-
kannte Exploits jahrelang nicht geflickt werden und viele Soft-
wareprogramme eine feindliche Übernahme so einfach machen
wie heute, solange bleibt es für Hacker leicht, im großen Stil
Daten abzugreifen. Das Zeitalter
der Massenhacks, so scheint es,
hat gerade erst begonnen.



Recht auf Verschlüsselung

In Deutschland wären Forderungen nach
einem Sonderzugang für Behörden zu ver-
schlüsselten Daten rechtlich äußerst zwei-
felhaft. „Das Grundrecht der Kommunika-
tionsfreiheit beinhaltet auch das Recht zur
Verschlüsselung, unabhängig davon, ob diese
Verschlüsselung auf technischem, semanti-
schem oder sonstigem Weg erfolgt“, sagt Dirk
Heckmann, Juraprofessor an der Universität
Passau und Mitglied des Bayerischen Ver-
fassungsgerichtshofes. „Dieses Grundrecht

darf durch staatliche Maßnahmen wie ein
Verschlüsselungsverbot, Sprachregelungen
oder die Pflicht der Bürger, einen Zweit-
schlüssel herauszugeben, nicht eingeschränkt
werden. Das wäre unverhältnismäßig.“

Die grundrechtlich festgeschriebene
Kommunikationsfreiheit umfasse auch die
elektronische Kommunikation: sei es Peer-
to-Peer, also direkt zwischen den Nutzern,
oder über einen Dritten, zum Beispiel einen

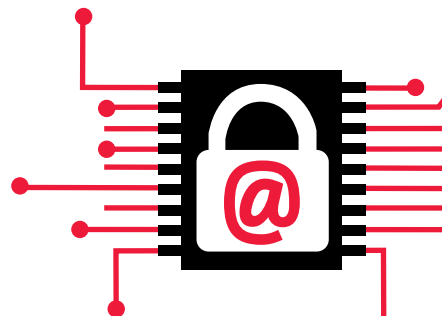
Mailprovider. „Der Staat darf dies nicht
generell unterbinden“, betont Heckmann, der
sich auf Sicherheits- und Internetrecht
spezialisiert hat. Wer technisch versiert genug
ist, kann seine Daten also ungehindert selbst
verschlüsseln, sodass der Schlüssel gar nicht
erst auf den Servern eines Serviceanbieters
wie der Telekom landet. Allerdings fehlt es
den meisten Nutzern am nötigen Wissen und
an einer Software, die dies standardmäßig
leistet.



» Die Deutschen haben das nicht drauf «

Für Thomas Rid vom Kings College London hat Deutschland nicht genug Know-how, um einen **Täter im Netz dingfest zu machen.**

INTERVIEW: CHRISTIAN HONEY



TECHNOLOGY REVIEW: Herr Rid, kann man die Quelle eines Hacks identifizieren?

RID: Attribution – also die Identifikation des Angreifers – und ihr Gegenteil, die Anonymität, führen, seit es Computerhacks gibt, eine Katz-und-Maus-Spiel. Lange hegten Sicherheitsforscher die Annahme, dass Hacker den Strafverfolgern technisch immer voraus sein werden – heute wird diese Ansicht stark hinterfragt. Denn es gibt immer mehr Fallbeispiele, in denen eine Attribution mit einer gewissen Sicherheit oder hoher Wahrscheinlichkeit möglich war. Die kurze Antwort lautet also: ja. Attribution ist aber eigentlich keine Ja-nein-Frage, sondern eine Frage der Abstufung. Wie gut die Identifikation des Angreifers in einem bestimmten Fall ist, darauf kommt es an.

Welchen Fährten kann man dafür folgen?

Für die Evidenz gibt es grob drei Ebenen: die technische, die operative und die strategisch-politische. Zur technischen Ebene gehört etwa Schadsoftware. Die kann man daraufhin analysieren, wie sie in das Zielsystem eingedrungen ist, welche Exploits dabei verwendet wurden und wie die gestohlenen Informationen verschlüsselt wurden. Zur operativen Ebene gehören etwa die Zeitzone und der zeitliche Ablauf des Angriffs. Zum Beispiel gibt es Fälle, bei denen sich herausstellte, dass der Angriff über die christlich-orthodoxen Feiertage an Weihnachten pausierte. Das ist natürlich ein starkes Indiz dafür, aus welcher Region der Welt der Angriff stammt. Um Antworten auf die Fragen auf der politisch-strategischen Ebene zu finden, braucht man auch nachrichtendienstliche Fähigkeiten, also zum Beispiel das Abhören eines Telefons oder den direkten Kontakt zu bestimmten Informanten. Selbst große Unternehmen können da nicht mithalten. Alles in allem sind die attributiven Fähigkeiten ungleich verteilt: Die Amerikaner haben das richtig drauf, die Deutschen nicht so.

Woran liegt das?

Wenn Sie Facebook, Dropbox und Google als Unternehmen haben, besitzen Sie einen riesigen Pool junger Leute, die sich in dem Feld sehr gut auskennen. Dann können Behörden wie die NSA natürlich wesentlich mehr machen, als wenn sie nur von Siemens und Mercedes rekrutieren können.

Wie viel Zeit kann eine Attribution beanspruchen?

Die Attribution erfordert sehr viel Kleinarbeit. Wie bei normalen Kriminalfällen dauert es oft Wochen, bis richtig klar geworden ist, in welcher Richtung man suchen muss.

Gibt es den perfekten Hack?

Wie den perfekten Einbruch kann es auch den perfekten Hack geben. Allerdings machen Menschen immer Fehler, vor allem wenn sie eine gewisse Routine haben. Irgendwann gibt es dann eine Technologie, die anhand kleiner Fehler auch den vormals perfekten Hack auffliegen lässt. Zum Beispiel bessere Intrusion-Detection-Software, die nicht nur den Informationsfluss in den und aus dem Rechner überwacht, sondern auch prüft, ob innerhalb des Netzwerks eine Anomalie auftaucht.

Was sind die größten Schwachstellen in Computersystemen?

Die Nutzer, nicht die Hardware. Das Grundproblem ist, dass die ganze Debatte ideologisch verbrämt ist. In Deutschland stellt sich etwa die Telekom hin und sagt: Sicherheit made in Germany ist besser als die von Google. Dieses Argument ist komplett lächerlich, auch weil viele US-Unternehmen in Reaktion auf Snowden ihre Sicherheit deutlich hochgefahren haben. Wie langsam die Umsetzung in Deutschland erfolgt, ist wirklich enttäuschend. Dort gibt es eine sehr hohe Zahl von Nutzern, denen die Fachkenntnis fehlt und die Sicherheitsentscheidungen stark ideologisch treffen. Das ist ein riesiges Problem aus meiner Sicht. Wenn sie ein Türschloss kaufen gehen und sich nicht nach der Qualität entscheiden, sondern danach, wo es hergestellt wird, ist das natürlich unsinnig. ☹



Thomas Rid forscht seit 2011 im Department of War Studies am King's College in London. Der Politologe hat sich auf Fahndungsmethoden spezialisiert, um die Täter hinter Cyber-Angriffen zu identifizieren.

Illustration: Jan Rieckhoff

Haben Sie was gegen Schnüffler?

Wir schon
>>>

ct
wissen

~~Überwachung~~

Das Praxishandbuch gegen Schnüffler

Sicherer Mail-Dienst:
12€ Rabatt Mindestbestellwert: ein Euro

ct Überwachung abwehren

Smartphones abdichten

Schnüffel-Apps ganz einfach zügeln
Lösungen für Unternehmen

Wirklich sicheres Online-Banking

Abhörsicher mailen

Sichere Mail-Services getestet
Komfortabel verschlüsseln



Jetzt für
nur **8,40 €**
bis 18.10. portofrei
bestellen.



shop.heise.de/ct-ueberwachung ✉ service@shop.heise.de
Auch als eMagazin erhältlich unter: shop.heise.de/ct-ueberwachung-pdf

Generell **portofreie Lieferung** für Heise Medien- oder Maker Media Zeitschriften-Abonnenten
oder ab einem Einkaufswert von 15 €



heise shop

shop.heise.de/ct-ueberwachung



Die Konkurrenz **liest mit**



Mit einer groß angelegten Internet-Fahndung will das FBI die fünf chinesischen Agenten Wang Dong, Huang Zhenyu (oben), Wen Xinyu, Sun Kailiang und Gu Chunhui (unten) der Cyber-Spionage überführt haben.



Die erste offizielle Anklage der USA gegen mutmaßlich staatlich geförderte Online-Spionage zeigt, **wie systematisch die Angreifer aus dem Netz vorgehen** – und wie schwer sich die Wirtschaft davor schützen kann.

VON DAVID TALBOT

Von einer Wand des FBI-Büros der US-Stadt Pittsburgh starren fünf Jungs aus Shanghai von einem „Wanted“-Poster. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu und Gu Chunhui sind laut einer im letzten Jahr entsiegelten Bundesanklage Agenten der chinesischen Volksbefreiungsarmee, Einheit 61398. Die fünf Gesuchten sollen sich in Netzwerke mehrerer amerikanischer Firmen gehackt haben, darunter U.S. Steel, Alcoa, Allegheny Technologies (ATI), Westinghouse, die US-Tochter des deutschen Photovoltaik-Produzenten Solarworld – und die größte nordamerikanische Industriergewerkschaft, United Steelworkers. Über mehrere Jahre hinweg, sagen die Staatsanwälte, stahlen die Agenten Tausende von E-Mails zur Geschäftsstrategie, Dokumente über Wettbewerbsklagen, die einige der US-Unternehmen gegen China eingereicht hatten, und sogar Kühlleitungspläne für Kernkraftwerke – alles angeblich zum Nutzen chinesischer Unternehmen.

Es ist die erste offizielle Anklage der Vereinigten Staaten gegen mutmaßlich staatlich geförderte Cyber-Spionage. Und sie hat Sicherheitslücken enthüllt, die Unternehmen selten öffentlich zugeben. Obwohl die Angreifer den Datenverkehr offenbar über die PCs unbeteiligter Nutzer umleiteten und ihre Aktivitäten auch anderweitig verschleierten, gelang es den Ermittlern, die virtuellen Einbrüche zu einem zwölfstöckigen Gebäude in Shanghai zurückzuverfolgen und einzelne Geheimdienstagenten zu identifizieren. Da die Vereinigten Staaten kein Auslieferungsabkommen mit China haben, gibt es wenig Chancen auf Festnahmen. Aber die US-Regierung hofft offenbar, die namentliche Nennung von Agenten – und die erfolgreiche Zurückverfolgung – werde China in Verlegenheit bringen, andere Nationen einschüchtern und zukünftige Wirtschaftsspionage damit bremsen.

Das mag unrealistisch sein. Sicherheitsunternehmen warnen weiterhin vor der Gefahr, und China nennt die Vorwürfe „völlig unbegründet und absurd“. Doch aus der Anklageschrift lässt sich eine weitere Lehre ziehen: Unternehmen können wertvolle Informationen online kaum noch sicher aufbewahren. Welche Maßnahmen sie auch immer ergreifen – mit den Bedrohungen halten sie nicht Schritt. „Offensichtlich hat sich die Situation verschlimmert, nicht verbessert“, sagt Virgil Gligor, Co-Direktor des Computersicherheitszentrums der Carnegie Mellon University (CyLab). „Wir haben den Zugang zu Diensten, Datenbanken und Konnektivität so bequem gemacht, dass er auch für unsere Gegner bequem ist.“ Sobald ein Unternehmen das akzeptiert, sagt Gligor, sei die naheliegendste Antwort eine drastische: die Verbindungen kappen.



Illustration: Alex Williamson

An einem kleinen Konferenztisch seines Büros am Pittsburgher Bundesgericht öffnet David Hickton einen von zu Hause mitgebrachten Behälter und köpft ein hart gekochtes Ei zum Mittagessen. Er ist der Bundesanwalt für West-Pennsylvania. Und obwohl er über eine Ermittlung mit Global Playern und undurchsichtigen Bedrohungen spricht, passt die eher bodenständige Atmosphäre: Der Fall spielt zum großen Teil in den eng verzahnten Kreisen der Pittsburgher Wirtschaft und Politik. Hickton deutet auf ein gerahmtes Foto. Auf dem Bild stehen er und ein Freund namens John Surma neben ihren Söhnen, die Eishockeykleidung tragen und gerade vom Eis gekommen sind. Beide Väter haben an der Universität Penn State studiert. Während Hickton die Hierarchie der Strafverfolgungsbehörden erklimmt, stieg Surma in der Unternehmenswelt auf und wurde CEO von U.S. Steel. Als Hickton 2010 leitender Bundesanwalt des Distrikts wurde, waren bei einem seiner Antrittsfrühstücke Surma und Leo Girard zu Gast, der Gewerkschaftsboss von United Steelworkers, die 1,2 Millionen aktive oder pensionierte Arbeiter mehrerer Branchen vertritt. „Ich wollte sie eigentlich bitten, in einem Gremium zur Prävention von Jugendkriminalität mitzuarbeiten“, erinnert sich Hickton. „Sie sagten: ‚Können wir über eine andere Angelegenheit sprechen?‘“

Zu der Zeit war der amerikanische Fracking-Boom in vollem Gange. Die sehr niedrigen Zinssätze befeuerten damals das Geschäft mit bis dahin unwirtschaftlichen Erdgas- und Öllagerstätten. Für deren Ausbeutung stellt U.S. Steel spezielle Rohrleitungen her. Sie sind sehr biegsam und haben keine vertikalen Nähte, weshalb sie sich unbeschadet Tausende Meter tief in die Erde rammen lassen. Dank der Rohre florierten die Umsätze bei U.S. Steel.

Doch dem Unternehmen waren zwei beunruhigende Entwicklungen aufgefallen. Erstens exportierten chinesische Staatsunternehmen große Mengen ähnlicher Rohre in die Vereinigten Staaten, zu niedrigen Preisen. U.S. Steel hatte daher Wettbewerbsbeschwerden beim US-Wirtschaftsministerium und der US International Trade Commission eingereicht mit der Begründung, der chinesische Staat subventioniere die Firmen. Die Verfahren führten letztendlich zu Sanktionen gegen China. Zweitens hatten sowohl U.S. Steel als auch die Gewerkschaft von verdächtigen E-Mails an Unternehmensmitarbeiter erfahren. Allerdings war unklar, wer dahintersteckte und ob ein Schaden eingetreten war. „Es gab ein allgemeines Bewusstsein für die Einbrüche, aber weder ein Wann, Wo noch Wie waren bekannt, ebenso wenig die Reichweite des Angriffs“, sagt Hickton.



Sun Kailiang soll am Klau Tausender Firmen-Mails beteiligt gewesen sein.

Illustration: Jan Rieckhoff

Die E-Mails waren äußerst geschickt formuliert. Sie gaben vor, von Kollegen oder Vorstandsmitgliedern zu stammen. Ihre Betreffzeilen nahmen Bezug auf Tagesordnungen für Meetings oder Marktforschungsergebnisse. Doch ihre Anhänge und die im Text enthaltenen Links dienten dazu, Malware einzuschleusen. Am 8. Februar 2010 etwa, so die Anklage, sendeten die Hacker eine E-Mail an mehrere Mitarbeiter von U.S. Steel – zwei Wochen vor einer Vorabentscheidung des Wirtschaftsministeriums. Sie schien vom CEO zu stammen, enthielt jedoch einen Link zu einer Website mit Malware. Einige Mitarbeiter klickten den Link an. Bald darauf wurden ihre Computer infiziert. Die Hacker stahlen Hostnamen für 1700 Server, die Zugänge zu Anlagen und Netzwerken des Unternehmens kontrollierten. Laut Anklage versuchte Cyberspion Wang Dong, diese Zugänge für seine Zwecke zu missbrauchen. Die Staatsanwaltschaft schweigt sich allerdings darüber aus, welche Informationen ausgelesen wurden.

Nach Aussage von Debbie Shon, Vizepräsidentin von U.S. Steel für den Bereich Handel, enthielten die Informationen wertvolle strategische Daten. „Es handelte sich nicht um Hightech-Blaupausen“, so Shon. „Doch die Informationen waren ebenso wichtig – Geschäftsstrategien, Preisgestaltung, Produktionsmengen sowie Zeitpunkt und Inhalt möglicher Wettbewerbsbeschwerden, die U.S. Steel als eines der größten Unternehmen seiner Sparte in Erwägung zog.“

In der Anklageschrift sind noch mehrere ähnliche Angriffe verzeichnet. Im Zeitraum von 2007 bis 2013 verhandelte etwa Westinghouse mit einem chinesischen Unternehmen über die Details eines Vertrags für den Bau von vier Atomreaktoren. Zwischen 2010 und 2012 stahl einer der Angeklagten von den Westinghouse-Computern angeblich mindestens 1,4 Gigabyte Daten – rund 700 000 Seiten E-Mails samt Anhängen. Die Dateien enthielten Rohrleitungspläne sowie eine E-Mail-Kommunikation, in der Westinghouse-Mitarbeiter ihre Sorgen über die chinesische Konkurrenz offenbarten.

Bei ATI stahlen die Hacker angeblich Passwörter von 7000 Mitarbeitern, während das Unternehmen in juristischen Auseinandersetzungen über seine Verkäufe in China steckte. Bei Alcoa entwendeten sie nach Angaben der Staatsanwaltschaft 2900 E-Mails mit mehr als 860 Anhängen, während sich die Firma in Vertragsverhandlungen mit chinesischen Unternehmen befand. (Alcoa, Westinghouse und ATI lehnten Stellungnahmen zu diesem Artikel ab.) Ein weiterer Angeklagter, Wen Xinyu, habe sich Zugang zu E-Mails mit internen Diskussionen der Gewerkschaftsführer verschafft, nachdem die Stahlarbeiter-

ct **Make:**

Leuchtschnur

- Arduino günstig nachbauen
- Blickfang: Unendlichkeitsspiegel
- Feuchtigkeitssensor aus Schreibwaren
- Materialkunde Klebstoffe

- Lärmampel für die Klasse
- Übersicht IC-Logikfamilien
- Bierbank-Skateboard

Wearables

Verstehen, nachbauen, angeben!
4 Projekte von leicht bis raffiniert

Leuchtfolie



Bock auf Basteln!

2x Make mit 35% Rabatt testen.

Ihre Vorteile:

- 2 Hefte mit 35% Rabatt testen
- Zusätzlich digital lesen über iPad oder Android-Geräte
- Zugriff auf Online-Artikel-Archiv*
- Versandkostenfrei

Für nur 12,90 Euro statt 19,80 Euro.

* Für die Laufzeit des Angebotes.



+ Artikel-Archiv



Jetzt bestellen und von den Vorteilen profitieren:
www.make-magazin.de/miniabo

Hier können Sie direkt bestellen und finden weitere Informationen.

Tel: 0541 80 009 125 E-Mail: leserservice@make-magazin.de
(Mo.-Fr. 8-19 Uhr, Sa. 10-14 Uhr)

Gewerkschaft 2012 begonnen hatte, die chinesische Industriepolitik öffentlich zu kritisieren.

Auch die US-Tochter von Solarworld war betroffen: Der deutsche Photovoltaik-Anbieter hatte Wettbewerbsverfahren mit der Begründung beantragt, chinesische Unternehmen verkauften Sonnenkollektoren unter Herstellungspreis und schmissen so ihre Rivalen aus dem Rennen. Eines Tages im Jahr 2012, erzählt Firmensprecher Ben Santarris, klingelte das Telefon im Solarworld-Büro in Camarillo, Kalifornien. Ein FBI-Mitarbeiter sagte, er und seine Kollegen hätten gestohlene Solarworld-E-Mails entdeckt. „Wir hatten keine Ahnung von diesen Vorgängen, bis der Anruf kam“, sagt Santarris. Erst als die Anklage im Mai 2014 entsiegelt wurde, erfuhr das Unternehmen den vollen Umfang des Diebstahls. „Die Angreifer hatten Zugang zu unserer Strategie für die Wettbewerbsverfahren, zu Unternehmenskennzahlen, Kosten, Gewinn- und Verlustrechnungen, Technologie-Roadmaps, Forschung und Entwicklung und so weiter“, sagt Santarris. Letztlich gewann das Unternehmen die Wettbewerbsverfahren, Strafzölle auf Einfuhren von Solaranlagen aus China waren die Folge. Während des Wettbewerbsstreits sei man sehr bemüht gewesen, den Verteiler entsprechender Informationen eng zu kontrollieren, so Santarris. „Zur gleichen Zeit, sagt das FBI, drang das chinesische Militär durch unsere Hintertür ein.“

Dass die Angriffe unbemerkt blieben, zeigt das erschütternde Versagen der vermeintlichen Sicherheitstechnologien. Lance Wyatt etwa, IT-Chef der Stahlarbeiter-Gewerkschaft, glaubte sich auf der sicheren Seite. Ein IT-Audit im Jahr 2010 hatte keine größeren Mängel festgestellt. Seine E-Mail-Server scannten alle eingehenden Nachrichten auf Anhänge, die ausführbaren Code enthielten. Er verwendete die neueste Antivirensoftware. Sein Netzwerk überprüfte IP-Adressen, um Websites mit Malware zu blockieren. Und doch fanden Wyatt und das FBI schließlich infizierte Computer. Einen davon nutzte der Leiter der Reisestelle. „Wir hatten keine dieser Maschinen als infiziert oder verdächtig auf dem Radar“, sagt Wyatt.

Laut Anklage nutzten die Hacker verschiedene Mittel zur Maskierung. Zum einen sollen sie bösartige E-Mails an Unternehmen und die Gewerkschaft von sogenannten

Illustration: Jan Rieckhoff



Wang Dong ist angeklagt, Server von U. S. Steel gehackt und Geschäftsunterlagen gestohlen zu haben.

Gu Chunhui steht unter Verdacht, Web-Attacken auf amerikanische Firmen mitorganisiert zu haben.

Illustration: Jan Rieckhoff



Hops aus gesendet haben. Darunter versteht man Computer unbeteiligter Nutzer, die Angreifer unter ihre Kontrolle bringen und als Zwischenstation verwenden. Einer stand beispielsweise in Kansas. Zweitens manipulierten sie geschickt das Internetsystem zur Benennung von Computeradressen. Die Hacker richteten Domainnamen wie „arrow service.net“ und „purpledaily.com“ ein und programmierten die Malware darauf, diese Domains zu kontaktieren. Nun konnten die Spione beliebig die Adressen der Server ändern, mit denen die Domainnamen verbunden waren.

Ideen für ein sicheres Internet kursieren zwar bereits seit Jahrzehnten. Akademische Forschungsinstitute und staatliche Labors haben immer wieder interessante Vorschläge gemacht. Doch nur sehr wenige dieser Ideen wurden umgesetzt. Sie erfordern breite Akzeptanz und nicht selten auch Kompromisse bei der Netzwerkleistung. „Man hört nicht mehr viel von einer Neukonzeption des Internets“, sagt Greg Shannon vom Software Engineering Institute der Carnegie Mellon University.

Unternehmen müssen sich also anders helfen. Wyatt etwa führte strengere Regeln bei United Steelworkers ein. Unter anderem gewährt er heute weniger Mitarbeitern sogenannte Administratorrechte für ihre PCs. Er durchsucht das Netzwerk nach verräterischen Anzeichen für Übertragungen durch Malware. Aber nichts davon hätte die Einbrüche verhindern können – es „hätte sie bestenfalls verlangsamt“, sagt Wyatt.

Die beste Option wäre vielleicht, sensible Daten vollständig vom Internet getrennt zu halten. Das hat Nachteile: Wenn E-Mail-Systeme nicht frei verwendbar sind oder Datenbanken offline bleiben, kostet es mehr Zeit für jeden einzelnen Nutzer, auf dem neuesten Stand zu bleiben. Sicherheitsexperten wie Vergil Gligor mahnen aber: „Wir müssen den Preis für die Sicherheit zahlen, und er besteht in Unbequemlichkeiten für uns selbst in Kauf nehmen, um große Hürden für die Angreifer zu errichten. Die beste Vorgehensweise dabei ist, gelegentlich offline zu gehen.“ ☘

c't Social Communication & Collaboration 2015

Soziale Netzwerke effizient nutzen
Unternehmenskommunikation intern und extern

Den Kundenkontakt müssen Unternehmen heute über alle Kanäle im Griff haben. Automatisierung hilft, Soziale Netzwerke effizienter zu nutzen. Bei der internen Kommunikation ist Struktur gefragt, um die Produktivität der Mitarbeiter zu sichern.

Frühbuchergebühr: 405,00 Euro (inkl. MwSt.)

Standardgebühr: 450,00 Euro (inkl. MwSt.)



VERANSTALTUNGSORT: KOMED in Köln

SAVE THE DATE:
18. November 2015

Themenschwerpunkte der Konferenz:

- **Web Experience:** Social Networks als Hilfsplattform im Business
- **Kundenkommunikation über alle Kanäle:** effizient und automatisiert
- **Social Networking:** in 7 Schritten zum Misserfolg
- **Interne Kommunikation:** Groupware versus Wikis, Whatsapp & Co.
- **E-Mail ist tot – lang lebe E-Mail:** Alternativen scheitern regelmäßig
- **Recht:** Datenschutz und Mitbestimmung in der Praxis
- **Strukturierte Kommunikation:** Ticketsystem statt Social Network

Sponsoren:



Universum AG
Digitale Lösungen



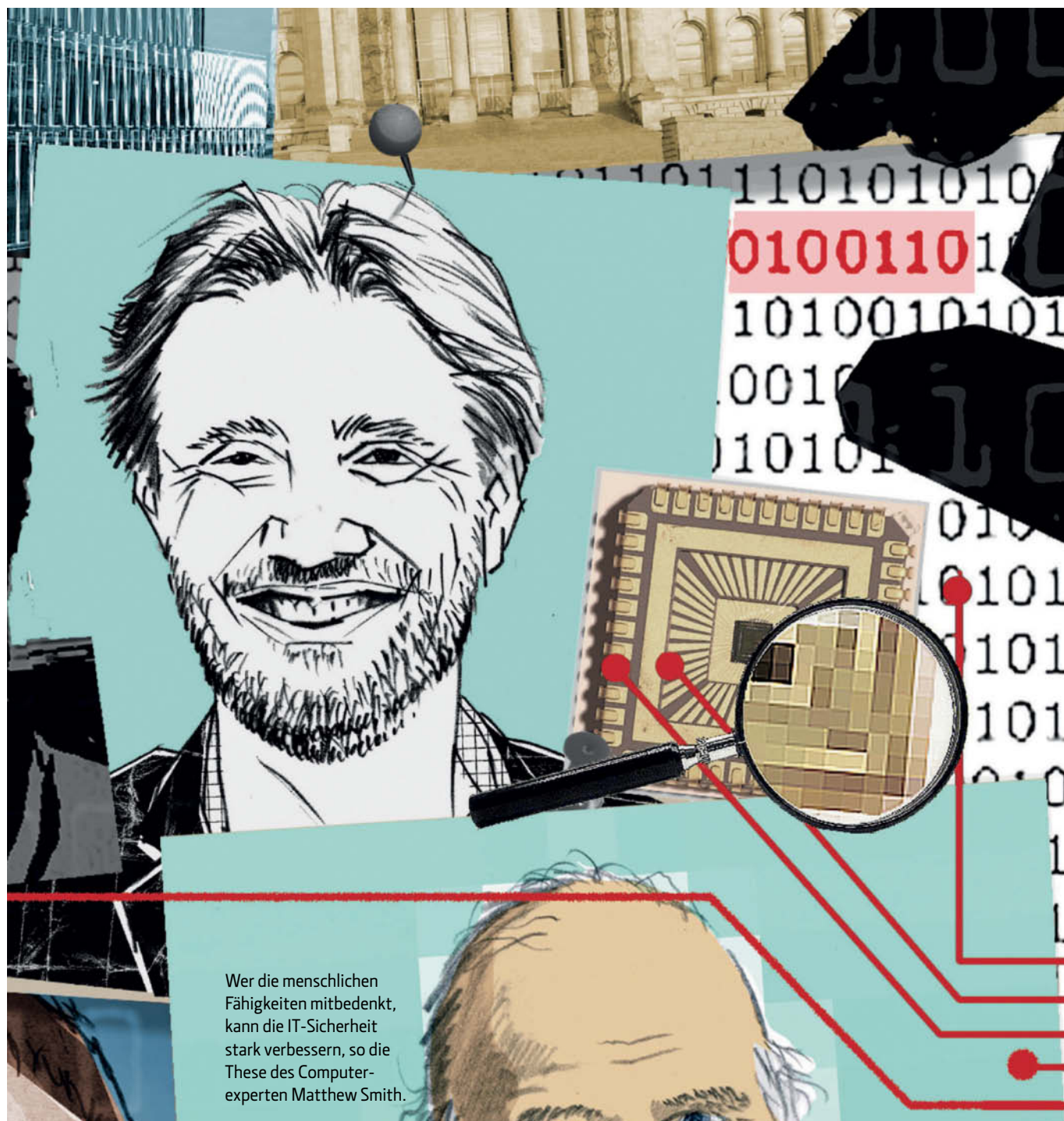
Zarafa
Open Source Email &
Collaboration Software

Organisiert von:



Weitere Informationen und Anmeldung unter: **www.heise-events.de/ctsocial2015**

Nutzen Sie die Möglichkeit zur PGP-Zertifizierung: **www.ct.de/pgp**



Wer die menschlichen Fähigkeiten mitbedenkt, kann die IT-Sicherheit stark verbessern, so die These des Computerexperten Matthew Smith.

Sicherheit **für jeden**

Lange Zeit hielten Informatiker den **Schutz vor Cyber-Attacken und Anwenderfreundlichkeit** für unvereinbar. Ein Irrtum.

VON EVA WOLFANGEL

Mantra eines Informatikers: „Lieber Nutzer, bitte verwende ein möglichst komplexes Passwort aus Buchstaben, Zahlen und Sonderzeichen, und nimm keinesfalls das gleiche für verschiedene Dienste!“ Lieblingsreaktion des Durchschnittsnutzers: „Okay, dann nehme ich 123mail für den Mail-Account, 123ebay für Ebay und 123amazon für Amazon.“ Kein Wunder, dass da manch ein Informatiker kapituliert. „Sicherheit wurde lange von Leuten entwickelt, die

nur die mathematische Seite gesehen haben“, erläutert Albrecht Schmidt vom Lehrstuhl für Mensch-Computer-Interaktion der Universität Stuttgart. Der Haken dabei: Kaum jemand kann sich komplexe Passwörter merken. „Mit dem Menschen im System gibt es keine absolute Sicherheit.“

Nach Überzeugung des Medieninformatikers Emanuel von Zezschwitz von der Ludwig-Maximilians-Universität München verschärft sich das Problem mit der wachsenden Zahl der mobilen Internetzugriffe noch weiter: „Passwörter auf dem Smartphone sind signifikant schlechter als auf dem Computer.“ Auf den kleinen Displays ist es den Nutzern schlicht zu aufwendig, Großbuchstaben oder gar Sonderzeichen zu verwenden. „Es muss leicht sein, komplexe Passwörter zu erstellen“, formuliert er deshalb als Sicherheitsanforderung für Mobilgeräte.

Das klingt zunächst wie ein unlösbares Paradoxon. Doch seitdem nicht nur Nutzer, sondern auch viele Computerexperten das Problem erkannt haben, arbeiten sie an neuen Strategien. Und siehe da: Sie finden Lösungen. Wer die menschlichen Fähigkeiten mitdenke, könne die Sicherheit enorm erhöhen, betont beispielsweise Matthew Smith, Leiter der Arbeitsgruppe Usable Security and Privacy an der Uni Bonn.

Dafür nutzen ließe sich etwa das motorische Gedächtnis der Menschen. Es speichert Bewegungen erstaunlich gut, was beispielsweise dazu führt, dass man Fahrradfahren nicht verlernt. Nutzer von PINs merken sich daher oft nicht die Zahlen, sondern die Bewegung, die ihr Finger vollzieht. Das erklärt, weshalb die Muster der Android-Geräte so beliebt sind. Nur: Auch Diebe können sich diese gut merken, wenn sie dem Handy-Besitzer im Bus oder in der U-Bahn über die Schulter schauen.

Dagegen könnte ein einfacher Trick helfen: Von Zezschwitz schlägt vor, die Mustereingabe auf die Rückseite des Smartphones zu verschieben. Da wir uns das Muster als Geste merken, müssen wir es beim Eingeben nicht sehen. Für eine Studie klebte er einfach zwei handelsübliche Smartphones aneinander: Die Nutzer waren zufrieden.

Diebe dürften auch verblüfft sein, wenn sie das Smartphone des Münchener Informatikers Alexander De Luca in die Hand bekommen – und trotz richtigem Muster keinen Zugriff auf die gespeicherten Daten erhalten. De Luca hat einen Algorithmus entwickelt, der auch die Art und Weise vergleicht, wie der

Nutzer das Muster zeichnet, beispielsweise seine Geschwindigkeit und den Druck auf das Display. Lediglich fünf Entsperrungen genügen dem System, um diesen biometrischen Faktor zu lernen – bis dahin gilt das Muster wie bei klassischen Android-Handys.

„Die meisten Probanden haben den zusätzlichen Faktor gar nicht bemerkt“, berichtet De Luca, „sie wurden nie abgewiesen.“ Die übrigen seien im Falle eines Fehlversuchs recht geduldig gewesen – eine Erkenntnis, die den Forscher zunächst verwunderte: Das Musterzeichnen dauert ohnehin deutlich länger als die Eingabe einer PIN. Wer beim ersten Versuch etwa wegen des Ruckelns der Straßenbahn abgewiesen wird, braucht noch länger. Wie passt das zur geringen Toleranz gegenüber Sicherheitsmaßnahmen? Solche Phänomene fasst De Luca unter den Begriff „Likeability“: „Musterzeichnen macht den Menschen einfach Spaß, sie mögen es.“ Im gleichen Maß wächst ihre Toleranz für Fehlversuche. Für den Fall, dass ein Nutzer beispielsweise aufgrund eines Gipsverbands sein Muster auf einmal völlig anders zeichnet, gibt es ein Masterpasswort – das dann allerdings wieder möglichst komplex sein müsste. Er sollte es ähnlich einer PUK an einer sicheren Stelle notieren.

Der Spaß könnte in Zukunft noch wachsen – und mit ihm die Sicherheit.

Denn die Informatiker denken schon an die nächste Dimension: Dank der Bewegungssensoren eines Smartphones wäre auch eine Authentifizierung möglich, indem etwa das gesamte Gerät

durch die Luft bewegt wird. Von Zezschwitz schlägt diesen Weg für Smartwatches

vor, auf deren winzigen Displays kaum andere sichere Authentifizierungsmöglichkeiten denkbar sind. Um sich anzumelden, bewegen Nutzer dann einfach ihren Arm nach einem bestimmten, selbst ausgedachten Muster. Studien zeigen, dass dreidimensionale Gesten nur schwer exakt nachzuahmen sind.

Auch die Kamera oder der Kompasssensor des Smartphones können solche Gesten wahrnehmen: Eiji Hayashi von der Carnegie Mellon University lässt seine Probanden ihrem Gerät zuwinken. Der Algorithmus erkennt via Kamera individuelle Faktoren wie Armlänge und typische Winkbewegung. Den Nutzern in seiner Studie machte das Spaß, die Fehlerquote war gering. Das Sicherheitskonzept des Stuttgarters Albrecht Schmidt stützt sich auf einen Magneten, mit dem Smartphone-Nutzer ihre Unterschrift in die Luft schreiben: Der Kompasssensor registriert die Signale und leitet sie an einen Algorithmus weiter, der die Ähnlichkeit der Unterschrift mit dem Original vergleicht. Auch dieses Verfahren erwies sich als zuverlässig: Beobachter konnten die Bewegung nicht gut genug imitieren, um das Handy zu entsperren, legitime Nutzer wurden meist auf Anhieb akzeptiert.

Schon klassische biometrische Merkmale wie ein Fingerabdruck erlauben, das Smartphone relativ zuverlässig und bequem zu sichern. Abdrücke wurden zwar in der Vergangenheit immer wieder gehackt. Das ist jedoch aufwendig und dürfte Otto-Normal-User eher selten treffen. Wenn es geschieht, dann ist das



Unsinnige Passwort-Regeln und überbordende Warnhinweise

Das Leben mit der Vielzahl an Passwörtern, die der Internetnutzer derzeit benötigt, lässt sich mit ein paar einfachen Tipps erleichtern. So sei es Unsinn, ein Passwort alle paar Wochen zu ändern, sagt Computerexperte Matthew Smith von der Uni Bonn. „Das verschlechtert die Nutzbarkeit und die Sicherheit.“ Um sich die häufig wechselnden Passwörter merken zu können, wählen die Nutzer meist einfachere und damit leichter entschlüsselbare Zahlen- und Buchstabenfolgen. Besser ist ein komplexes Passwort, das man sich über eine Eselsbrücke merkt und lange Zeit verwendet. Zudem brauchen nur manche Webseiten ein besonders sicheres Passwort, allen voran der E-Mail-Account. Denn über ihn kann ein Datendieb an die Passwörter für viele andere Dienste gelangen. Er braucht nur zu behaupten, er habe sein altes Passwort vergessen – und um ein neues bitten. Die Dienste schicken dem Nutzer das angeforderte neue Passwort dann in der Regel per E-Mail zu. Beim Schutz der Mailbox lohne sich also ein wenig Aufwand, so Smith: „Schlechte Passwörter sind eines der Haupteinfallstore – auch für die Geheimdienste.“

Ein zweites auffälliges Ärgernis sind die ständigen Warnungen vor Webseiten mit nicht vertrauenswürdigen Zertifikat. Sie werden meist von den Nutzern ignoriert. Zum einen sind sie kaum verständlich. „Selbst Sicherheitsexperten können häufig nicht erkennen, ob eine Gefahr davon ausgeht, auf ‚OK‘ zu klicken“, sagt Smith. Ein wichtiger Grund für die Missachtung dürfte jedoch sein, dass die Warnungen so oft kommen – und bei Missachtung meist nichts passiert. Viele Nutzer nehmen sie nicht mehr ernst und haben in der Regel damit sogar recht, weil die Warnungen schwer zu programmieren und deshalb häufig fehlerhaft sind. Im Schnitt verbirgt sich nach Smiths Berechnungen nur hinter einer von 15 400 Zertifikatswarnungen ein Angriff. Vor diesem Hintergrund „sollte man sie eigentlich abschaffen“, sagt Smith. Sie scheinen jedoch einen anderen Vorteil zu haben: Als sich Smith mit Edward Snowden über technische Details der Ausspähungen austauschte, erfuhr er, dass die Warnungen Geheimdienste vor entsprechenden Attacken abhalten: Die Chance, entdeckt zu werden, schreckt die Spionageprofis ab – auch wenn das Risiko gering ist. Selbst bei einer Fehlerquote von 1:15 400 ist es also gut, sie nicht komplett zu übergehen.

Mit der steigenden Zahl mobiler Internetzugriffe erhöhe sich das Sicherheitsrisiko deutlich, warnt der Medieninformatiker Emanuel von Zezschwitz.



Illustrationen: Jan Rieckhoff

allerdings ungeschickt: Ein solches Passwort lässt sich der Fingerzahl entsprechend nur neunmal ändern. Forscher sehen daher in erweiterten biometrischen Faktoren die Zukunft: Beispielsweise könnte unsere Art zu gehen mobilen Geräten helfen, ihre legitimen Benutzer zu identifizieren, ebenso unsere üblichen Aufenthaltsorte oder genutzten Apps. Das Smartphone könnte so erkennen, wenn etwas auffällig anders ist, und nur dann nach einem Passwort fragen – das der Nutzer möglichst komplex erstellen und gut gesichert aufbewahren sollte. Er wird es so gut wie nie benötigen, prophezeien die Forscher.

„Wir sollten in Zukunft adaptiver werden“, fordert von Zezschwitz: „Den Nutzer nur dann nerven, wenn es nötig ist.“ Denn die Zeit, die jeder mit dem Entsperren seines Handys verbringt, wächst: In einer Studie der Münchener Informatiker verwendeten Nutzer durchschnittlich eine Stunde im Monat auf Musterzeichnen, Powernutzer gar neun Stunden. Häufig brauchten sie das Gerät dann nur für wenige Sekunden.

Mit einer ausgeklügelten Zugangssperre für Smartphones ist es allerdings nicht getan. Auch Apps sind ein Sicherheitsproblem, das viele offenbar unterschätzen. Sie erhalten allzu leicht Zugriff auf private Daten. Nach Beobachtungen des Bonner Sicherheitsexperten Matthew Smith akzeptieren Nutzer in der Regel alle Zugriffsrechte einer App, ohne sich klarzumachen, was das bedeutet. Die Hauptursache sei mangelnde Transparenz. Smith visualisierte daher die sonst nur per Text kommunizierten Zugriffsrechte im Installationsprozess: Wollte eine App den Standort wissen, meldete das System sinngemäß: „Du befindest dich jetzt in der Hauptstraße 7 in Stuttgart-Feuerbach – das weiß die App künftig auch“, der Zugriff auf die Kontaktdaten wurde mittels eines Fotos, etwa der Großmutter des Nutzers, visualisiert. „Die Leute gehen unter solchen Bedingungen signifikant bewusster mit ihrer Privatsphäre um“, sagt Smith.

Eines bleibt trotz all dieser Ideen zwar bestehen: Hundertprozentige Sicherheit wird es auch mit ihnen nicht geben. Aber „80 Prozent gelebte Sicherheit sind besser als 100 Prozent Sicherheit, die keiner nutzt“, sagt Smith.

c't Mobile 2015



Foto: © ra2 studio – Fotolia.com

„Mobile Geräte im Unternehmen“ Sicher einbinden – produktiv einsetzen

BYOD ist in vielen Unternehmen bereits Alltag, bei der sauberen Trennung von privaten und geschäftlichen Daten hapert es aber nach wie vor. Doch Sicherheit allein genügt nicht, Mobility muss auch die Produktivität der Mitarbeiter steigern – und sollte den Kunden besser einbinden.

Frühbuchergebühr: 382,50 Euro (inkl. MwSt.)

Standardgebühr: 450,00 Euro (inkl. MwSt.)

VERANSTALTUNGSORT: KOMED in Köln

**19.
November
–
Köln**

Themenvorschau:

- Berufliches & Privates in einem Gerät – aber sauber getrennt
- iOS im Unternehmenseinsatz – einfach verwalten und absichern
- Enterprise Mobility & Apps – aus Mitarbeiter und Kundensicht
- Praxis: Mobilität managen, Produktivität steigern
- Android im Unternehmen – Neuer Vorstoß: „Google for Work“
- Recht: SW-Lizenzmanagement für BYOD, virtuelle Desktops & Cloud

Goldsponsoren:



Silbersponsor:



Organisiert von:





Gut, aber gesetzwidrig?

Ethische Hacker decken im Auftrag von Unternehmen Sicherheitslücken auf. Ein gefragter Dienst, doch die Anbieter solcher Hilfsleistungen bewegen sich in einer legalen Grauzone.

VON BERND MÜLLER

Hilfe, ich bin gehackt worden.“ Solche Mails hat Karsten Nohl früher mehrmals am Tag bekommen. Heute nicht mehr, denn seine Mail-Adresse und Telefonnummer gibt der 34-Jährige nur noch Vertrauten und Kunden, seine Firma Security Research Labs firmiert lediglich unter einer Berliner Postadresse. SRL unterstützt Unternehmen dabei, Sicherheitslücken in ihrer Software aufzuspüren. Nohl und sein kleines Team knacken im Kundenauftrag Passwörter, verschicken Phishing-Mails an ahnungslose Mitarbeiter oder untersuchen neue Sicherheitslücken, wie zuletzt „BadUSB“, die Entdeckung, dass sich jedes USB-Gerät – vom Speicherstick bis zur Webcam – zu einer USB-Tastatur umprogrammieren lässt, die Schadsoftware in einen Rechner schleust.

Als Elektrotechnikstudent hat Karsten Nohl festgestellt, dass er gern Verschlüsselungsverfahren „kaputtmacht“. Statt auf die schiefe Bahn zu geraten, wurde er einer von den Guten: ein „ethischer Hacker“, im Gegensatz zu den bösen Hackern, die im Verborgenen arbeiten und Sicherheitslücken an Kriminelle verkaufen, nicht selten zu sechsstelligen Preisen. Die Szene boomt: Zahlreiche Firmen helfen Unternehmen, Sicherheitslücken zu finden, größere Unternehmen beschäftigen sogar eigene Hacker – zu Spitzengehältern.

Aber selbst sie sind nicht unbedingt sicher vor Strafverfolgung. Sie bewegen sich in einem rechtlichen Graubereich. Laut Paragraph 202c des Strafgesetzbuchs, auch Hackerparagraph genannt, macht sich jeder durch das „Vorbereiten des Ausspähens und Abfangens von Daten“ strafbar – selbst wenn er im Auftrag des Besitzers der Daten handelt. Den Hackerparagraphen hatte der Deutsche Bundestag im Mai 2007 mit großer Mehrheit verabschiedet. Dass dieses Gesetz bisher noch nie zur Anwendung kam, liegt schlicht daran, dass kein Auftraggeber ein Interesse daran hat, seinen Dienstleister an den Pranger zu stellen.

Das aber muss keineswegs immer so bleiben. Karsten Nohl plädiert deshalb für eine Anpassung oder gar Abschaffung des Paragraphen: „Andernfalls können wir mit den kriminellen

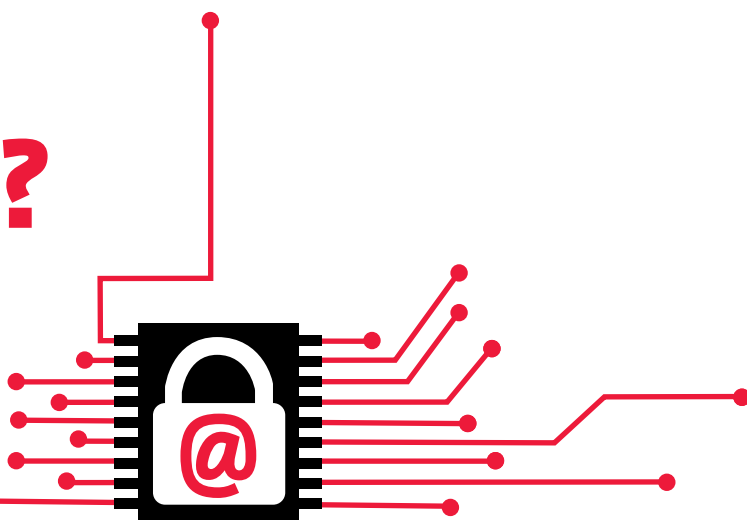
Hackern nicht Schritt halten, und die Sicherheitsforschung würde ins Ausland abwandern.“

Eric Bodden sieht das ähnlich. Der Professor am Fraunhofer-Institut für Sichere Informationstechnik in Darmstadt untersucht unter anderem Kryptoalgorithmen, etwa zum Schutz von Festplatteninhalten, oder die Sicherheit eingebetteter Software, also von Programmen, die Smartphones, TV-Geräte oder Autos steuern. „Wir finden oft Lücken“, sagt Bodden. Hundertprozentig legal ist auch seine Tätigkeit nicht.

Behindert sieht sich der Wissenschaftler insbesondere beim generellen Verbot des Reverse Engineering, das man im weiteren Sinne als Rückübersetzen von Software beschreiben könnte. Informatiker rekonstruieren aus der laufenden Software die zugrunde liegenden Programmierbefehle. Auf diese Weise können Sicherheitsforscher Einfallstore für Hacker leichter finden. Doch das Reverse Engineering ist verboten, weil Produktpiraten komplexe Software und die Funktionen von elektronischen Markenprodukten leichter nachbauen können, wenn sie die Entwicklungsgeschichte zurückverfolgen.

Diese Begründung findet Bodden völlig unangemessen: Software unterliegt nämlich dem Urheberrecht, ist also etwa einem Roman gleichgestellt und darf ohnehin nicht verändert werden, auch ohne zusätzlichen gesetzlichen Schutz. Als Folge kann der Fraunhofer-Forscher Reverse Engineering bei kommerzieller Software nur mit ausdrücklicher Genehmigung des Herstellers betreiben. Entsprechend viele Programme mit Sicherheitslücken dürften den Sicherheitsexperten entgehen.

Ein wesentliches Einfallstor würden jedoch auch diese Methoden nicht schließen. Einfachstes Angriffsziel sind nämlich leichtsinnige Mitarbeiter, die ahnungslos eine Mail aufklicken, die scheinbar eine Besprechungsnotiz vom letzten Meeting, tatsächlich aber Spähsoftware enthält. Mit ein paar Stunden Recherche lasse sich eine täuschend echte Mail mit hoher Erfolgsquote fabrizieren, so Karsten Nohls Erfahrung. „Wenn ich fünf Mails verschicke, klickt mindestens einer drauf und



installiert, ohne es zu wissen, einen Virus.“ Damit sie den Fehler nicht wiederholen, führt Nohl den überführten Mitarbeitern anschließend ein Video vor, das sie auf die Tragweite ihres Fehlklicks hinweist und Vorschläge für einen verantwortungsvolleren Umgang mit dem IT-System macht. Gegenüber der Geschäftsleitung des Unternehmens bleiben die Betroffenen aber anonym.

Von ähnlichen Erfolgsquoten bei vorsätzlichen Täuschungsmanövern berichtet Christian Bruns, Manager für Cyber-Sicherheit beim Oldenburger IT-Berater BTC. Auf ein gut gemachtes digitales Fax klickten in Phishing-Kampagnen mehr als die Hälfte der überrumpelten Personen. Das BTC-Hacker-Team testet Webseiten von Energieunternehmen auf Schwachstellen, zunehmend prüfen sie kritische Infrastrukturen, etwa Kommunikationsmodems von Photovoltaikanlagen oder anderen dezentralen Energieanlagen. „Alle unsere Hacker unterschreiben eine Verpflichtung, ihr Wissen nur in Abstimmung und im Sinne unserer Kunden anzuwenden“, betont Christian Bruns.

In dieser Funktion dürfen sie auch keine Software-Schwachstellen von anderen Hackern kaufen, die damit Geld verdienen wollen, weder in Form von Viren oder Trojanern, noch in Form von Wissen über neu entdeckte, aber noch geheime Sicherheitslücken. Und erst recht verkaufen sie ihr eigenes Wissen um einen Sicherheitsmangel nicht an Kriminelle. Sie stellen es vielmehr frei zur Verfügung oder bieten ihre Kenntnis dem Unternehmen an, das von dem Fehler betroffen ist. Findet ein ethischer Hacker beispielsweise eine Schwachstelle in Windows, wird er seine Entdeckung kostenlos weitergeben oder an Microsoft verkaufen, das dann die Lücke stopfen kann.



Dass es für solche Deals einen lukrativen Markt gibt, ist bekannt. Der Markt für dunkle Geschäfte rund um die Softwarefehler sei jedoch noch wesentlich lukrativer, sagt Karsten Nohl. „Deshalb versuchen wir, Sicherheitslücken als Erste zu finden und den Kriminellen die Geschäftsbasis zu entziehen.“



meinung



Runter vom Sockel

Die Idee, dass die Geschichte von herausragenden Einzelpersonen vorangetrieben wird, ist längst widerlegt. In der Technologiebranche aber lebt dieser Mythos weiter – und er ist schädlich.

Know-how für Linux-Profis

Seit dem Tod von Steve Jobs 2011 ist Elon Musk zur wichtigsten Berühmtheit des Silicon Valley geworden. Er hat es nicht nur auf die Titelseiten von „Fortune“ und „Time“ sowie auf die Liste der „größten Erfinder von heute“ des „Atlantic“-Magazins geschafft – er diente dem Hollywood-Star Robert Downey jr. sogar als Inspiration für seine Darstellung des Superhelden „Iron Man“.

Musks Unternehmen Tesla Motors und SpaceX haben in der Tat das Potenzial, ihre Branchen grundlegend zu verändern. Doch die Geschichten über Musks Rolle dabei klingen merkwürdig überholt. Die Vorstellung von „Great Men“, die den Wandel quasi im Alleingang vorantreiben, stammt aus dem 19. Jahrhundert. Heute glauben die meisten Wissenschaftshistoriker nicht mehr an den einsamen Erfinder. Selbst herausragende Persönlichkeiten brauchen ein Umfeld, das Ressourcen und Chancen bietet.

Auch Musks Erfolg wäre ohne staatlich finanzierte Grundlagenforschung und Subventionen nicht möglich gewesen. Er hat von einer langen Reihe früherer Innovationen profitiert. Trotzdem hält sich das Heldenbild bei Journalisten und Wagniskapitalgebern hartnäckig. Das ist nicht nur unfair gegenüber anderen Menschen, die ebenfalls ihren Beitrag zu neuen Technologien geleistet haben. Es verzerrt obendrein die Vorstellung der Öffentlichkeit darüber, wie neue Technologien entstehen – und untergraben so die Strukturen für künftige Innovationen.


Nach Studien der Physik und Ökonomie zählte Musk 1995 zu den Gründern eines Unternehmens namens Zip2, das Online-Landkarten für Unternehmen anbot. Er war zwar nicht der eleganteste Programmierer, doch er arbeitete rund um die Uhr und schlief „auf einem Sitzsack neben seinem Schreibtisch“, wie Ashlee Vance in seiner Musk-Biografie (siehe TR 6/2015, S. 38) schreibt. „Musk war bereit, seine Existenz für den Aufbau dieser Plattform aufs Spiel zu setzen“, zitiert Vance einen früheren Mitarbeiter. 1999 übernahm Compaq die Firma, und Musk beteiligte sich an der Gründung eines Finanzdienstleisters, aus dem später PayPal werden sollte. Laut Vance begann er an diesem Punkt, „seinen typischen Stil zu entwickeln – in ein ultrakomplexes Geschäft einsteigen und sich dabei nicht im Geringsten daran stören, dass er nicht viel über seine Feinheiten weiß“.

Als PayPal 2002 für 1,5 Milliarden Dollar an Ebay

verkauft wurde, hatte Musk genug Geld für seine Leidenschaften. Er investierte mehr als 100 Millionen Dollar aus eigenem Vermögen in das Raumfahrtunternehmen SpaceX und gründete gleichzeitig Tesla. Mit den Jahren kultivierte er in den Medien seine Persönlichkeit als „halb Playboy, halb Weltraum-Cowboy“, so Vance.

Musk verkauft sich als einen Mann, der im Alleingang Berge versetzt, und lässt andere nur ungern an seinen Lorbeeren teilhaben. Bei SpaceX wurden die Ingenieure „jedes Mal kollektiv wütend, wenn Musk in Interviews wieder einmal behauptete, die Falcon-Rakete mehr oder weniger allein konstruiert zu haben“, schreibt Vance. Dabei ist Musk



 shop.heise.de/linux-2015

 service@shop.heise.de

Auch als eMagazin erhältlich unter:
shop.heise.de/linux-2015-pdf

Jetzt für
nur **9,90 €**
bestellen.

Generell **portofreie Lieferung**
für Heise Medien- oder Maker Media
Zeitschriften-Abonnenten oder ab
einem Einkaufswert von 15 €

 **heise shop**

shop.heise.de/linux-2015



angewiesen auf Menschen, die mehr Ahnung von Autos und Raketen haben als er selbst – und vielleicht auch mehr soziales Geschick. Wer unter Musk überlebt, ist meist ein Arbeitstier und bereit, auf öffentliche Anerkennung zu verzichten. Bei SpaceX gibt es dafür Gwynne Shotwell, die den laufenden Betrieb leitet, bei Tesla den Chief Technology Officer JB Straubel, der bedeutende technische Fortschritte verantwortet. Sie bleiben stets im Schatten.

Dort bleibt auch die Rolle des Staats. Wenn sich Musk mal wieder über die Nasa aufregt, wirkt er geradezu wahnhaft. „SpaceX profitiert von Jahren und Jahren staatlich finanzierter Technologie und öffentlicher Förderung“, sagt Mariana Mazzucato, Ökonomin an der University of Sussex. Als SpaceX 2008 nach drei gescheiterten Versuchen die erste Rakete in die Luft brachte, reichte das aus, um von der Nasa Aufträge über 1,6 Milliarden Dollar zu bekommen. Noch Jahre später beruht das Geschäft von SpaceX weitgehend auf öffentlichen Aufträgen. Auch seine Technologie ist zu guten Teilen aus staatlich finanzierten Projekten entstanden. Das soll nicht etwa bedeuten, dass SpaceX keine eigenen Innovationen beigesteuert hätte. Es hat Raketenstarts zum Beispiel deutlich billiger gemacht. Aber dabei profitiert es von Technologien und bestens ausgebildeten Menschen, die es schon vorher gab.

Ähnlich ist die Lage bei Tesla. Lithium-Ionen-Batterien etwa wurden in den späten 1980er-Jahren mit hohen Zuschüssen des US-Energieministeriums und der National Science Foundation entwickelt. Außerdem hat Tesla erheblich von Kreditgarantien und Subventionen profitiert: 2010 erhielt es vom Energieministerium etwa eine Kreditzusage über 465 Millionen Dollar und von Nevada, wo Musk eine „Gigafactory“ für Batterien errichtet, 1,29 Milliarden Dollar an Steuererleichterungen. Hinzu kommen laut „Los Angeles Times“ noch einmal eine Milliarde Dollar an weiteren Krediten und Steuernachlässen sowie Subventionen für die Kunden. Gegenüber CNBC sagte Musk immerhin, die Subventionen seien zwar nicht erforderlich, aber dennoch „hilfreich“ gewesen. Er beharrt also mehr oder weniger darauf, dass staatliche Unterstützung keine große Rolle in seiner Erfolgsgeschichte spielt.

Für Musks Selbstbezogenheit gibt es ein berühmtes Vorbild: Steve Jobs. So wie sich Musk obsessiv um die Türgriffe oder Touchscreens der Tesla-Wagen kümmert, so brachte auch Jobs leidenschaftliche Intensität in das Produktdesign ein. Aber für die wichtigsten technischen Funktionen von Macs, iPods oder iPhones war Jobs nicht selbst verantwortlich. Eine korrekte Version der Apple-Story würde die Beiträge anderer – etwa von Designer Jonathan Ive – stärker würdigen. Und den historischen Kontext: „Es gibt keine einzige Schlüsseltechnologie hinter dem iPhone, die nicht staatlich finanziert gewesen wäre“, schreibt die Ökonomin Mazzucato – etwa Mobilfunk, Internet, GPS, Touchscreens oder Sprachtechnologie. Apple hat diese

Technologien zwar auf ebenso neuartige wie beeindruckende Weise miteinander kombiniert. Doch sie beruhen auf vielen Jahren staatlich finanzierter Vorarbeit. Glauben wir wirklich, dass es ohne Musk und Jobs heute keinen Smartphone-Boom und kein Interesse an Elektroautos gäbe?

Diese Frage ist wichtig, denn das Superman-Gerede bringt erhebliche Kosten mit sich. Zunächst einmal beschädigt es die Kultur des Silicon Valley, indem es als Entschuldigung für fürchterliches Verhalten gilt. Musk ist bekannt dafür, leichtfertig Ingenieure zu demütigen und Mitarbeiter zu feuern. Als seine Assistentin, die Tesla und SpaceX zwölf Jahre ihres Lebens gewidmet hat, 2012 um eine Gehaltserhöhung bat, ließ er sie kurzerhand gehen. Nicht einmal rein geschäftlich gesehen ist Musks Gnadenlosigkeit wirklich nützlich, denn sie gefährdet die überlebenswichtigen Beziehungen zu staatlichen Stellen. Musks größter Feind werde „immer er selbst und sein Umgang mit Menschen“ sein, sagte ein früherer Beamter im Gespräch mit Vance.

Ähnlich war auch Jobs für kaltes und anmaßendes Auftreten gegenüber Mitarbeitern bekannt. „Diese Bösartigkeit war nicht nötig“, schreibt Walter Isaacson in seiner Jobs-Biografie. „Sie hat ihm mehr geschadet als geholfen.“ Wenn das Silicon Valley weiterhin talentierte Menschen anziehen möchte, wären motivierendere Management-Praktiken sicherlich hilfreich.

Heldenmythen sind noch auf andere Weise schädlich: Gelten Technologie-Leitfiguren als singuläre Einzelkämpfer, können sie leichter einen unangemessenen Anteil am Gewinn einstreichen, statt ihn durch den Verzicht auf Steuertricks teilweise wieder zurück an Agenturen wie die Nasa oder die National Science Foundation fließen zu lassen.

Und zuletzt: Die Anbetung von Technikhelden kann unsere Visionen für die Zukunft verzerren. Warum sollte der Staat beispielsweise den öffentlichen kalifornischen Personenverkehr ausbauen, wenn Musk behauptet, man könne Menschen mit 1200 Kilometern pro Stunde durch einen „Hyperloop“ (siehe TR 5/2015, S. 16) jagen? Eine Gesellschaft muss ihre langfristigen Prioritäten im Technologiebereich selbst bestimmen, ohne dabei den persönlichen Visionen einiger Stars übermäßiges Gewicht einzuräumen.

Statt also die Technologie-Leitfiguren auf ein Podest zu stellen, sollten wir die Rolle des Staates bei der Finanzierung von Grundlagenforschung und als Partner für neue Vorhaben stärker würdigen. Wer die Bedeutung öffentlicher Investitionen herunterredet, erschwert zukünftige Innovationen.



**>> Heldenmythen untergraben
künftige Innovationen. <<**

AMANDA SCHAFFER ist freie Journalistin und schreibt für „Slate“, die „New York Times“ und andere Publikationen über Wissenschaft und Medizin.

GNADENLOS DURCHLEUCHTET.

THEMEN UND TESTS MIT LEIDENSCHAFT.

4x
c't PLUS
FÜR 14,20 €*



JETZT 2 MONATE DAS c't-PLUSABO TESTEN:

- 4x c't als **HEFT + DIGITAL****
+ Online-Zugriff auf das **ARTIKEL-ARCHIV**
für nur 14,20 €*
- Bereits **freitags** lesen
- Nach der Testphase erwartet Sie die
c't-NETZWERKKARTE mit exklusiven
Vorteilen.

IHR GESCHENK: **POWERBANK**

Für Ihre Testbestellung bedanken wir uns mit
der **Powerbank 5.000mAh** als Stromreserve für
unterwegs (für Smartphones und Tablets).

Sie sind bereits Abonnent und möchten für 18,20 € auf das
Plus-Abo umsteigen? Unser Leserservice hilft Ihnen gern
beim Wechsel – mit einer
Powerbank als Dankeschön.

ct.de/plusabo

0541/80 009 120

leserservice@heise.de

Bitte bei Bestellung angeben: 1CEA1501

*Preis in Dt. inkl. MwSt. Auslandspreise können abweichen.

**Verfügbar für Android (Tablet, Smartphone, Kindle Fire) und iOS (iPad, iPhone)

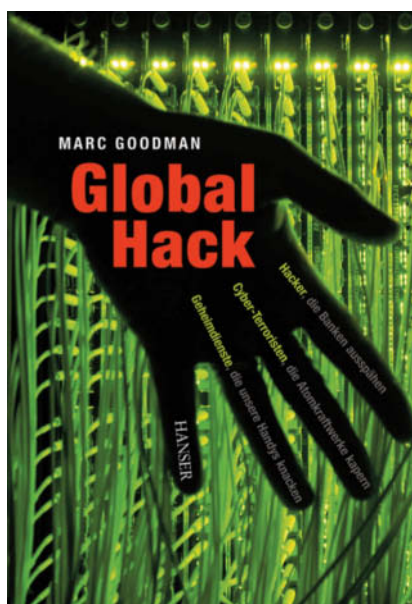
Folgen Sie uns auf:





Alles wird schlimm

Marc Goodman schreibt über die Verbrechen der Zukunft und wie wir uns dagegen schützen können.



MARC GOODMAN: GLOBAL HACK

Carl Hanser Verlag, 600 Seiten, 24,90 Euro

Der Klappentext führt ein wenig in die Irre: „Bestens ausgebildete Elite-Kriminelle“, heißt es da, „mischen neben Terrororganisationen, Geheimdiensten und ausländischen Regierungen immer öfter mit beim globalen Daten-Monopoly. Das Internet wendet sich gegen uns. Es wird Zeit, dass wir aufwachen.“ Aber der erste Eindruck täuscht. In „Global Hack“ geht es um mehr als Hacker, die Banken ausspähen, und Geheimdienste, die

unsere Handys knacken: Im zweiten Teil des Buches – und das ist der sehr viel spannendere – geht es vor allem um die Zukunft des Verbrechens.

„Was die rein technische Bedrohung unserer Sicherheit angeht, so ist die Zukunft längst da“, schreibt Goodman. „Sie erwacht gerade im Laptop des Jugendlichen neben Ihnen in der Bibliothek, der die nächste Silk Road und den nächsten Assassination Market gründet. Sie lauert in der Garage eines hasserfüllten Biohackers, der es leid ist, in der Schule gehänselt zu werden, und es jetzt seinen Klassenkameraden mit dem neuen Bakterienstamm mal so richtig zeigen will. Sie stapelt sich beim Discounter, der Quadrocopter-Drohnen im Sonderangebot feilbietet, die ohne Murren auch Waffen über Gefängnismauern und Flughafenzäune tragen.“

Neben der Bedrohung durch Malware und der alltäglichen Überwachung durch Smartphones und Big Data diskutiert Goodman die zahlreichen Möglichkeiten, die sich Verbrechern bieten, wenn sie technisch auf der Höhe der Zeit sind. Angefangen bei Drohnen, über Funkjammern, die elektronische Schlösser, Alarmanlagen und GPS-Module außer Gefecht setzen, über die kreative Nutzung von 3D-Druckern für kriminelle Zwecke bis hin zu den Möglichkeiten böser Biohacker.

Natürlich ist dieser Teil des Buches hoch spekulativ – obwohl Goodman die einzelnen Abschnitte mit zahlreichen Fußnoten unterfüttert. Und der Autor ist notorisch pessimistisch: Auch wenn beispielsweise nicht klar ist, ob Biohacker in Zukunft wirklich maßgeschneiderte Biowaffen entwerfen, die gezielt einzelne Personen töten

könnten, geht Goodman immer vom Schlimmsten aus. „Alle Warnzeichen sind da, die Lage ist ernst, und wir dürfen keine Zeit mehr verlieren“, schreibt er. „Ich darf Ihnen versichern, dass die Kriminellen, die Terroristen, die anderen bösen Jungs ganz gewiss keine Zeit verlieren.“

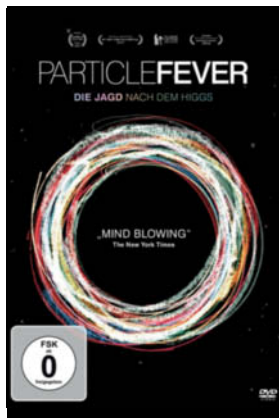
Dennoch sind die Vorschläge Goodmans zur Lösung der Misere spannend und bedenkenswert – gerade weil der Autor der festen Überzeugung ist, dass Polizei und Ermittlungsbehörden zurzeit dabei sind, das technische Wettrennen mit den Verbrechern dieser Welt zu verlieren. Denn was dem ehemaligen Mitarbeiter des FBI vor-schwebt, ist eine Art Crowdsourcing gegen das Verbrechen. Freiwillige



» Die bösen Jungs werden ganz sicher keine Zeit verlieren. «

Helfer beispielsweise könnten in einer Art Spiele-Umgebung Phishing-E-Mails ansehen und versuchen, in Echtzeit betrügerischen Spam zu identifizieren. „Es gibt einen Weg aus der Masse der technischen Bedrohungen“, schreibt Goodman. „Indem wir den einfachen Bürger mobilisieren und uns die Kontrolle über unsere eigenen Geräte zurückholen, können wir das Potenzial aller zum allgemeinen Besten ausnutzen.“ Da wechselt der Pessimismus in Idealismus. Trotzdem ist zu hoffen, dass er recht behält.

WOLFGANG STIELER



PHYSIK Es bleibt spannend

Bitte nicht mehr als 140 Gigaelektronen-volt. Hätte das Higgs-Boson eine höhere Masse, wäre das ein starkes Indiz für die „Multiversum“-Theorie. Die ist vielen Physikern ein Graus, weil sie bedeuten würde: Auch der stärkste Teilchenbeschleuniger kann dem Universum kaum noch neue Erkenntnisse abtrotzen.

Die physikalischen Hintergründe reißt die Doku „Particle Fever“ nur an. Regisseur Mark Levinson interessiert sich mehr für die Menschen dahinter. Über Jahre hinweg hat er ihre Suche nach dem Higgs-Boson begleitet. Das Ergebnis ist ein spannender Einblick in die Leidenschaften, Frustrationen und Rivalitäten der beteiligten Physiker.

Die Masse des Higgs-Bosons nutzt er dabei geschickt als Spannungsbogen, denn die Freunde der „Supersymmetrie“-Theorie wünschen sich maximal 115 GeV. Als der Large Hadron Collider in Genf endlich die ersten Messdaten ausspuckt, sind sie geschockt: Die Werte deuten auf irgendetwas im Bereich von 140 GeV hin. Der krimiähnliche Show-down kulminiert in der legendären Konferenz vom 4. Juli 2012, auf der zwei unabhängige Teams ihre Ergebnisse bekanntgeben: rund 125 GeV. Damit bleiben viele Fragen offen und die Physik spannend.

GREGOR HONSEL



BIOLOGIE Schlaues Gemüse

Sind Pflanzen intelligent? Mit dieser provokanten Frage spannt Stefano Mancuso einen großen Bogen über das Leben von Bäumen, Blumen und Gemüse. Als Pflanzenforscher und Professor an der Universität Florenz erzählt er von vielen Fähigkeiten, die vor allem botanisch unkundige Leser noch nie gehört haben dürften: „So schließen viele Blumen ihre Blüten, wenn sie von Insekten besucht werden, und lassen sie erst wieder frei, wenn diese mit Pollen beladen sind.“ Sie besitzen also einen Tastsinn.

Mancuso listet zudem Beispiele für Licht-, Hör- „und noch 15 weitere Sinne“ auf. Das ist spannend zu lesen, leicht verständlich geschrieben – auch wenn er die Pflanzen bisweilen zu betont als unterschätzte Lebewesen darstellt. Aber folgt aus den Fähigkeiten wirklich, dass Pflanzen intelligent sind? Mancuso meint selbstredend Ja – und greift dafür zur denkbar umfassendsten Definition: „Intelligenz ist die Fähigkeit zum Problemlösen“. Diese Fähigkeit jedoch hat jedes Lebewesen, sonst hätte es nicht überlebt. Der provokante Titel wird zur Allerweltserkenntnis. Einen Nebeneffekt hat die Lektüre allerdings: Sie macht klar, wie unbestimmt der Begriff Intelligenz eigentlich ist.

ROBERT THIELICKE



PSYCHOLOGIE Die Kraft der Farben

Blau beruhigt, Rot regt an: Alles schon mal gehört? Zum Glück bietet das Thema Farben aber weit mehr Interessantes und Kurioses, wie der französische Farbdesigner Jean-Gabriel Causse in seinem unterhaltsamen Buch beweist. Warum sind zum Beispiel New Yorker Taxis gelb-schwarz? Weil Bremsen und Federung der frühen schwarzen Taxis weniger zuverlässig waren als heute und häufig Unfälle verursachten. Damit man sie besser sieht, ließ der Taxiunternehmer John Hertz seine Wagen in den beiden kontrastreichsten Farben lackieren. Beispiel zwei: Blaue Würfel fühlen sich wärmer an als rote, obwohl sie dieselbe Temperatur haben. Das Gehirn überkompensiert offenbar die Erwartung, dass blaue Objekte kälter seien.

Causse erklärt auch, warum Pharma- und Lebensmittelunternehmen die Farbwahl nicht dem Zufall überlassen: Grüne Beruhigungsmittel wirken stärker als rote, und die Eignung von Wasser für Babynahrung signalisiert man am besten mit Rosa. All das garniert Causse sparsam mit den physikalischen Grundlagen der Farbwahrnehmung.

Allerdings enthält das Buch bis auf die schicke Farboxplosion auf dem Cover unverständlicherweise keine Abbildungen.

VERONIKA SZENTPÉTERY

Mark Levinson: „Particle Fever – Die Jagd nach dem Higgs“, Blu-ray-DVD, 99 Minuten, 13,99 Euro

Stefano Mancuso, Alessandra Viola: „Die Intelligenz der Pflanzen“, Verlag Antje Kunstmann, 19,95 Euro

Jean-Gabriel Causse: „Die unglaubliche Kraft der Farben“, Hanser Verlag, 192 Seiten, 19,90 Euro



karriere

Ramazan Sütmen
plant und betreut
Netzwerke bei
VW.



Beruf:

Netzwerkarchitekt

Die IT-Netze von Volkswagen verbinden fast zweieinhalb Millionen Menschen miteinander: 600 000 im Konzern, 1,2 Millionen bei den Zulieferern und 650 000 bei den Händlern. Der Autobauer betreibt weltweit zehn Rechenzentren. „Ohne unsere Netzwerke würde kein Auto die Fabrik verlassen“, sagt Harald Berg, Leiter IT Tools, Network und Data Center bei VW. „Sie sind die Lebensadern des Konzerns.“

In der Wolfsburger Zentrale kümmern sich zwölf Netzwerkarchitekten um diese Adern. Einer von ihnen ist Ramazan Sütmen, 45. Nach einer Ausbildung zum Energieanlagenelektroniker hat er an der Fachhochschule

Wolfenbüttel technische Informatik mit Schwerpunkt Datenkommunikation studiert. Seit 2011 ist er bei VW schwerpunktmäßig für Netzwerksicherheit zuständig. „Funktionale Anforderungen und Sicherheit gehen bei Netzwerken meist Hand in Hand“, sagt Sütmen. Daher kennt er sich mit beidem aus.

Zurzeit bereitet er Netzwerkstrukturen für die Kommunikation zwischen Autos und VW-Servern vor. 2020 werden wohl nahezu alle Neufahrzeuge internetfähig sein, schätzt Sütmen. Also muss er die nötige Leistungsfähigkeit des Netzwerks berechnen sowie die nötigen Server, Router und Firewalls aussuchen.

Jede größere Änderung an den Netzwerken setzt zahlreiche Abstimmungen mit den verschiedenen Fachabteilungen voraus. „Wir diskutieren dann intensiv über die bestmögliche Lösung“, sagt Sütmen. Er und seine Kollegen brauchen also reichlich Kommunikationstalent und Teamfähigkeit. Dazu kommt noch das technische Handwerkzeug. Das erwirbt er vor allem durch Berufserfahrung und stetige Weiterqualifizierung.

Wenn das Netzwerk steht, schließen andere Abteilungen Schritt für Schritt ihre Server an. „Das geht Hand in Hand“, sagt Sütmen. Da Netzwerke wachsen und leben, müssen deren Architekten auch künftige

Immer mehr Geräte vom Feuermelder bis zum Auto erhalten einen Internetanschluss. Netzwerkarchitekten kümmern sich darum.

Entwicklungen stets im Blick haben. „Netzwerkarchitekten sorgen dafür, dass die Netzwerke nicht nur technisch funktionieren, sondern im Idealfall auch betriebswirtschaftlich“, sagt Johannes Weickel vom Branchenverband Bitkom. Je cleverer ein Netzwerk aufgebaut ist und je weniger Wartung es braucht, umso günstiger ist es im Betrieb.

PETER ILC

NETZWERKARCHITEKT

AUSBILDUNG: Studium der Informatik oder Elektrotechnik

ARBEITSMARKT:

steigender Bedarf

EINSTIEGSGEHALT:

40 000 bis 45 000 Euro

Foto: VW

MASTERSTUDIENGANG Fachleute für komplexe IT-Infrastrukturen

Zum Wintersemester startet an der Fachhochschule Kiel der neue Masterstudiengang „Information Engineering“, ein gemeinsames Angebot der Fachbereiche Informatik, Elektrotechnik und Wirtschaft. Mit der Einführung reagiert die Hochschule auf Anforderungen des Arbeitsmarkts: Unternehmen suchen verstärkt Fachleute für komplexe IT-Infrastrukturen. Deren Aufgabenfeld beinhaltet neben klassischen Softwareentwicklungen längst auch die Abwehr von Industriespionage, den Schutz geistigen Eigentums und der Privatsphäre sowie die wirtschaftliche Organisation von Unternehmen.

Diesen Trend berücksichtigt der viersemestrige englischsprachige Masterstudiengang mit den vier Schwerpunkten Intelligent Systems, IT-Security, „Information Technology and Systems Development“ sowie Business-IT-Management. Studenten lernen zum Beispiel, komplexe Systeme selbstständig zu konzipieren und zu entwickeln sowie IT-Sicherheit mess- und überprüfbar zu machen. Absolventen können eine Karriere im IT-, Banken- und Versicherungssektor verfolgen. Die Bewerbungs- und Einschreibefrist endet am

15. Oktober 2015. V. SZENTPÉTERY **LINK** www.fh-kiel.de/studienangebot

MINT-NACHWUCHS Schüler programmieren Roboterhände

Wie können haarfeine Drähte Roboterhände zum Leben erwecken? Wie funktionieren künstliche Muskeln? Diese Fragen beantworteten Stefan Seelecke und sein Team in einem neuen Schülerangebot an der Saar-Uni. Damit soll der künftige Nachwuchs früh für ein Studium der Ingenieurwissenschaften begeistert werden. An je einem Tag vor Ort können die Schüler einen mit Formgedächtnisdrähten als Muskeln betriebenen Mini-Roboterarm bauen und so programmieren, dass er präzise kleine Aufträge ausführt „Dabei erhalten sie einen Einblick, was erforderlich ist, um ein solches System zu bauen: von der Antriebstechnik über Aktorik und Sensorik bis hin zur Programmierung eines Mikrocontrollers, sodass der Arm die Kugeln mit exaktem Timing abwirft“, erläutert Seelecke. Anmelden können sich Schüler ab der elften Klasse.

VERONIKA SZENTPÉTERY

STUDIE Generation Y falsch eingeschätzt?

Traumtänzer, die keine Lust auf eine große Karriere haben und eine Auszeit nach der anderen nehmen – diese Einschätzung über die Generation Y ist ein Klischee. So zumindest eine Studie des Kienbaum Institut @ ISM für Leadership und Transformation. Das Institut identifizierte bei einer Befragung von 600 Hochschulabsolventen vier Typen (siehe Grafik).

Karriereorientierte (20 Prozent) und Ambitionierte (38 Prozent) gehören demnach zu den Berufseinsteigern, bei denen Arbeitgeber mit klassischen Karriereangeboten punkten können: Für sie hat Karriere und beruflicher Erfolg nach wie vor einen hohen Stellenwert, der Leistungswille ist sehr ausgeprägt. Der Unterschied: Für Ambitionierte, die die größte Gruppe bilden, spielen Erfolg und Karriere auch eine große Rolle, werden aber nicht gegenüber der Familie und Work-Life-Balance priori-

siert. Erlebnisorientierte (29 Prozent) und Orientierungssuchende (13 Prozent) gehören dagegen zu den Berufseinsteigern, für die die Erwerbstätigkeit derzeit keinen großen Stellenwert in der Lebensplanung einräumt und die keine Führungsposition anstreben. Für Erlebnisorientierte stehen Familie und Freunde an erster Stelle der Werteskala.

Von ihrem zukünftigen Arbeitgeber erwarten sie Weiterbildungsmöglichkeiten und eine abwechslungsreiche Tätigkeit in kollegialer Arbeitsatmosphäre mit flachen Hierarchien. Orientierungssuchende wiederum erhoffen sich vom Arbeitgeber klare Vorgaben und Weiterbildungsmöglichkeiten, um die eigenen Ziele herauszufinden. V. SZENTPÉTERY

Die vier Typen der Generation Y

Die Mehrheit der Absolventen will Karriere machen.

38 %

Ambitionierte

♀ 52 %

♂ 48 %

29 %

Erlebnisorientierte

♀ 36 %

♂ 64 %

20 %

Karriereorientierte

♀ 33 %

♂ 67 %

13 %

Orientierungssuchende

♀ 54 %

♂ 46 %

Quelle: Kienbaum Institut@ISM, 2015

POSTLEITZAHL 0



01217 Dresden

Elektronik, Produktions-/ Automatisierungstechnik, Life-Sciences, Green Economy

TechnologieZentrumDresden GmbH

3 Standorte für Ihr Technologieunternehmen. Kompetenz für Start-Ups und Wachstum.

Dr. B. Dressel

Tel.: 03 51/8 71 86 65

Fax: 03 51/8 71 87 34

E-Mail: kontakt@tздresden.de

www.tздresden.de



06766 Bitterfeld-Wolfen, OT Wolfen

Chemie, Beschichtungs- und Schichtbildungstechnologie, Photovoltaik, Fotophysik, Fotochemie, nachwachsende Rohstoffe/ neue Materialien, Weiße Biotechnologie

Technologie- und Gründerzentrum Bitterfeld-Wolfen GmbH

Technologiezentrum im Chemiepark Bitterfeld-Wolfen

Tel.: 0 34 94-63 83 00

Fax: 0 34 94-63 83 02

E-Mail: info@tgz-chemie.de

www.tgz-chemie.de

POSTLEITZAHL 1



12459 Berlin

Optische Technologien, Gerätetechnik, Informationstechnologie, Medizintechnik, Maschinenbau

TGS Technologie- und Gründerzentrum Spreeknä

Netzwerkpartner in der Technologieregion

Berlin-Südost mit individuellen

Betreuungsangeboten, Ostendstr. 25,

SEK GmbH, Anja Reimann

Tel.: 030/5304 1000, Fax: 030/5304 1010,

E-Mail: info.tgs@tgs-berlin.de

www.tgs-berlin.de



12489 Berlin

Biotechnologie, Informationstechnologie, Optische Technologien, Mikrosystemtechnologie, Erneuerbare Energien

Wissenschafts- und Technologiepark Berlin Adlershof

Werden Sie Mitglied der einzigartigen Wissenschafts- und Business-Community Adlershofs: 6 Institute der Humboldt-Universität, 10 außer-universitäre Forschungseinrichtungen, 1.000 Unternehmen, 15.500 Beschäftigte und 9.500 Studenten. Adlershof. Science at Work.

WISTA-MANAGEMENT GMBH,

Dr. Peer Ambrée, Rudower Chaussee 17

Tel.: 030/6392 2250

E-Mail: ambree@wista.de, www.adlershof.de



12555 Berlin

Umwelttechnik, -technologie, Optoelektronik, Verfahrenstechnik, Biotechnologie, Medizintechnik

Innovationspark Wuhlheide Berlin

Netzwerkpartner in der Technologieregion Berlin Südost mit individuellen Betreuungsangeboten

IMG mbH, Köpenicker Str. 325,

Carola Reiblich

Tel.: 0 30/65 76 24 31

Fax: 0 30/ 65 76 27 99

E-Mail: img@ipw-berlin.de, www.ipw-berlin.de

POSTLEITZAHL 2



23562 Lünebeck

Medizintechnik/-produkte, Life Sciences, Optical/Vision Technologies, Informatik, Robotik

BioMedTec-Campus Lünebeck

Einzigartige gemeinsame Location der Profil-Universität, University of Applied Science / Fachhochschule, Fraunhofer Marine Biotechnologie sowie Medical Vision, UKSH Universitätsklinikum mit Transfer-/Experimental-OP, zusammen mit mehreren Multifunktionscentern für Gründer, junge Technologiefirmen und Entwicklungs-/ Projektbüros etablierter Unternehmen in der „Stadt der Wissenschaft“ Lünebeck

Tel.: 0171/530 9668

E-Mail: mildner@unitransferklinik.de

www.tzl.de

www.unitransferklinik.de

POSTLEITZAHL 3



34131 Kassel

Produktions-/Verfahrenstechnik, Technische Dienstleistungen, Informationstechnologie

FIDT Fördergesellschaft für innovative Dienstleistungen und Techniken mbH

Top-Standort für den Einstieg in den Markt, Perfekte Verkehrsanbindung. Breitband-IT-Infrastruktur, flexible Flächen von 13-200 m², vernetzt im Haus und in der Region.

Tel.: 0561/93897-0

www.fidt.de

POSTLEITZAHL 4



40225 Düsseldorf

Biotechnologie, Medizintechnik, Chemie/Pharma, Umweltschutz

Life Science Center Düsseldorf

Büros und Labore (bis S2-Standard) für Existenzgründer & etablierte High-Tech-Firmen und Dienstleister; Universitätsnähe; Netzwerk von Experten aus Wissenschaft, Wirtschaft & Finanzen

Dr. Thomas Heck

Tel.: 0211/6022460,

E-Mail: heck@lsc-dus.de, www.lsc-dus.de

UNSER SERVICE FÜR TECHNOLOGIEPARTNER

Die Rubrik „Technologiepartner“ ist eine Plattform für Technologie- und Gründerzentren sowie für Technologieparks. Als Technologie- und Gründerzentrum haben Sie die Möglichkeit, die Leser von Technology Review auf Ihr Zentrum und Ihre Dienstleistungen aufmerksam zu machen.

POSTLEITZAHL 5



50829 Köln

Biotechnologie/Pharma, Medizintechnik, Chemie, IKT, Cleantech

BioCampus Cologne Grundbesitz GmbH & Co. KG

Der BioCampus Cologne entwickelt sich zu einem der größten Biotechnologieparks Deutschlands. Vom Gründer bis zum Global Player finden hier innovative Unternehmen optimale Wachstumsbedingungen und eine perfekte Infrastruktur.

Andre van Hall

Tel.: 0221/168095 90

Fax: 0221/168095 99

E-Mail: info@biocampuscologne.de

www.biocampuscologne.de



Rechtsrheinisches Technologie- und Gründerzentrum Köln GmbH

51105 Köln

Biotechnologie, Informationstechnologie, Medizintechnik, Verfahrenstechnik, Design

RTZ Rechtsrheinisches Technologie- und Gründerzentrum Köln GmbH

Zeit und Raum für Gründer mit Ideen; Infrastruktur – multifunktional und flexibel; Coaching, Beratung, Service und Netzwerke für High-Tech-Start-ups auf dem Hagen-Campus in Köln

Dr. Heinz Bettmann

Tel.: 0221/83911-0, Fax: 0221/83911-11

E-Mail: info@rtz.de, www.rtz.de

Facebook: www.facebook.com/RTZkoeln

POSTLEITZAHL 6



67059 Ludwigshafen

Chemie, Pharma, Nano-, Biotechnologie, alle chemiebasierten Technologien

chem2biz im TZL – TechnologieZentrum Ludwigshafen am Rhein GmbH

Unterstützung und Zugang zum chem2biz-Netzwerk. Räumlichkeiten, Services, Gründungs- und Wachstumsberatung für Gründer und junge Unternehmen.

E-Mail: info@chem2biz.de

Tel.: 0621/5953-0,

www.chem2biz.de



69120 Heidelberg

Biotechnologie, Informatik, Medizin, Organische Elektronik, Pharma, Umwelttechnik
Technologiepark Heidelberg GmbH
Büros und Labore für Unternehmen und Existenzgründer, Beratung, internationales Netzwerk aus Wissenschaft, Wirtschaft und Bildung

- Internationaler PartnerPort mit Büro vor Ort
- ConferenceCenter

Tel.: 06221/5025710, Fax: 06221/5025711

E-Mail: info@technologiepark-heidelberg.de

www.technologiepark-heidelberg.de

www.heidelberg-startup-partners.de

POSTLEITZAHL 9



91522 Ansbach

Umweltschutz/-technik, Technische Dienstleistungen, Informationstechnologie
Technologie- und Innovationszentrum Ansbach

Individueller Ausbau - Büros ab 16 m²

Tel.: 0981/953838-0, Fax: 0981/953838-38

E-Mail: info@tiz-ansbach.de

www.tiz-ansbach.de



96450 Coburg

Maschinenbau, Informationstechnologie, Kultur- und Kreativwirtschaft
Wir vernetzen dynamische Unternehmen in Coburg. Inspirierendes Umfeld mit Tagungslocation. Attraktive Büroräume. Verbindung zur Wirtschaftsförderung. Hochschulnah. Ausgezeichnetes innovatives Konzept.

designwerkstatt coburg

Am Hofbräuhaus 1

96450 Coburg

Tel.: +49 9561 83630, Fax: +49 9561 8363-119

E-Mail: info@designwerkstatt-coburg.de

www.designwerkstatt-coburg.de

Heise Medien GmbH & Co. KG
Technology Review Anzeigen
Karl-Wiechert-Allee 10 · 30625 Hannover

Fax: 05 11/53 52-3 08
E-Mail: julia.gabel@heise.de
Tel.: 05 11/53 52-5 71

TECHNOLOGY REVIEW: ANGEBOT FÜR TECHNOLOGIEPARTNER

Mit einem Eintrag unter der Rubrik „Technologiepartner“ haben Sie monatlich die Möglichkeit, die Leser von Technology Review auf Ihr Zentrum/Ihre Dienstleistungen aufmerksam zu machen. Ihr Angebot wird nach Postleitzahlen sortiert aufgenommen. Für einen Jahreseintrag (5 Zeilen à 40 Zeichen + Logo) berechnen wir exklusiv nur 1200 Euro (zzgl. MwSt.). Gerne sende ich Ihnen Informationen und Unterlagen zu, ich freue mich auf Ihre Anfrage.

29. 09 – 30. 09. 2015, HAUS DER TECHNIK, ESSEN

4TH CONFERENCE ON CO2 AS FEEDSTOCK FOR FUELS, CHEMISTRY AND POLYMERS

Wie kann der Bedarf an Treibstoffen und Chemikalien im Jahr 2050 gedeckt werden? Mehr als 200 internationale Experten diskutieren dies vor dem Hintergrund bahnbrechender neuer Methoden im Bereich von Carbon Capture and Utilization (CCU) auf der diesjährigen größten europäischen Konferenz.

www.co2-chemistry.eu

29. 10. 2015, TUTTLINGEN

7. INNOVATION FORUM "MEDIZINTECHNIK"

Die Plattform zur Präsentation innovativer Ideen, Technologien, Prototypen, Konzepte und Herstellungsverfahren im Bereich der Medizintechnik

www.technologymountains.de/medizintechnik

06. 11. 2015, HANNOVER

2015 – DAS JAHR DER MRK: PERSPEKTIVEN DER MENSCH-ROBOTER-KOLLABORATION

Die wachsende Autonomie moderner Robotersysteme fordert bisherige Grenzziehungen, Rollen und Normen im Verhältnis zwischen Menschen und Maschinen heraus. Aus diesem Anlass lädt der Technik-Salon, Leibniz Universität Hannover, zu einem interdisziplinären Dialog zwischen Hightech-Forschung und -Industrie und den Sozial- und Rechtswissenschaften ein.

www.technik-salon.de/mrk-tagung

12. 11. 2015, REGENSBURG

2. Kooperationsforum mit Fachausstellung HOLZ ALS NEUER WERKSTOFF

Innovationen mit holzbasierten Materialien
Fach- und branchenübergreifende Vernetzung von Akteuren, die Holz für neue Einsatzbereiche herstellen und nutzen möchten – das ist Ziel des zweiten Kooperationsforum „Holz als neuer Werkstoff“. Vorgestellt werden Strategien und Marktperspektiven, wie u. a. Marktstudien und –erfahrungen. Schwerpunktthemen sind Holz als Basis für High-Tech-Werkstoffe mit neuen Anwendungspotenzialen sowie zukunftsweisende Technologien und Produktlösungen, wie beispielsweise additive Fertigung, Carbontechnologie, Wertschöpfung aus Rinde und Bionik.

www.bayern-innovativ.de/werkstoffholz2015

25. 11. 2015, BAYREUTH

Kooperationsforum mit Fachausstellung FUNKTIONELLE INHALTSSTOFFE

Die Bayern Innovativ konzipiert und organisiert im Rahmen des Netzwerks Life Science das 4. Kooperationsforum "Funktionelle Inhaltsstoffe" in Zusammenarbeit mit der Universität Bayreuth. Der Themenfokus liegt auf Trends und Perspektiven für funktionelle Inhaltsstoffe, Identifizierung und Gewinnung von Inhaltsstoffen für Food und Kosmetik, Bioaktivität, moderne Analytik und Food Safety, Anwendungen in Verpackung und Textil sowie 3D-Food Printing und Industrie 4.0 Konzepte im Lebensmittelsektor.

Das Forum bietet Kontakte zu Partnern aus Industrie und Wissenschaft; es soll Entwickler, Hersteller und Anwender von Inhalts- bzw. Naturstoffen mit Vertretern aus verschiedenen Wirtschaftssektoren wie Lebensmittel, Kosmetika, Verpackungsmaterialien und Textil zusammenführen.

<http://www.bayern-innovativ.de/ingredients2015>

24. 11.–26. 11. 2015, NÜRNBERG

SPS IPC DRIVES

Elektrische Automatisierung - Systeme & Komponenten - Internationale Fachmesse

www.mesago.de/sps

26. 11. 2015, DÜSSELDORF

NEXT ECONOMY AWARD: DEUTSCHLANDS PREIS FÜR GRÜNE GRÜNDER

2015 vergibt die Stiftung Deutscher Nachhaltigkeitspreis die erste nationale Auszeichnung für Startups, die auf Nachhaltigkeit und die Green Economy setzen.

Die Verleihung des Next Economy Awards findet am 26. November im MARITIM Hotel Düsseldorf nach einem Live-Pitch statt.

www.nexteconomyaward.de

16. 12.–17. 12. 2015, MARITIM HOTEL, KÖLN

SIXTH WPC CONFERENCE, COLOGNE

WOOD AND NATURAL FIBRE COMPOSITES

Die in diesem Jahr weltweit größte Konferenz zu Wood-Plastic Composites (WPC) zeigt mit der Erweiterung um naturfaserverstärkte Kunststoffe (NFK) sowie bio-basierte Polymere aktuelle Trends und Wachstumsbereiche an neuen Märkten auf, plus: die weltgrößte WPC- und NFK- Ausstellung.

www.wpc-conference.com

INFORMIEREN SIE DIE LESER VON TECHNOLOGY REVIEW ÜBER IHRE VERANSTALTUNGEN UND KONGRESSE.

Ansprechpartner: Julia Gäbel, Telefon: 05 11/53 52-571, Fax: 05 11/53 52-308, E-Mail: julia.gabel@heise.de



Wachsende Zweifel

An dieser Stelle blicken wir zurück auf Artikel, die vor fünf Jahren in Technology Review erschienen sind.

Diesmal: **Fracking**



TECHNOLOGY REVIEW 10/2010
Stellt Schiefergas die globale Energieversorgung auf den Kopf?

In Schiefer-Lagerstätten in den USA sind riesige Mengen Erdgas gefunden worden. „Die Entdeckung hat einen Boom in den USA ausgelöst, und sie könnte auch die Energieversorgung in Europa völlig umkrempeln“, schrieb TR in der Titelgeschichte der Ausgabe 10/2010. „Doch die neue Option ist nicht ohne Risiken.“

Die „Option“, von der dort die Rede ist, diskutierten seinerzeit in Europa höchstens Fachkreise: Die Förderung von „nichtkonventionellem Gas“ im großen

Stil. Denn das Unterfangen ist technisch sehr aufwendig. Um ein Feld auszubeuten, sind sehr viele Bohrstellen nötig, die Bohrungen müssen über weite Strecken horizontal verlaufen – vor allem aber muss man fracken, also das Muttergestein aufbrechen, indem man unter hohem Druck eine Frack-Flüssigkeit einpumpt.

Die amerikanische Ölindustrie setzte dennoch kompromisslos auf diese Option. 2009, berichtete TR, habe das Potential Gas Committee (PGC), ein Expertengremium aus Industrie und Forschung, die Höhe der Gasresourcen der USA auf insgesamt 59 Billionen Kubikmeter geschätzt – rund ein Drittel davon nichtkonventionell. Mittlerweile taxiert das Gremium sie auf 71 Billionen Kubikmeter. Die U.S. Energy Information Administration (EIA) rechnet damit, dass die Förderung von Erdgas in den USA bis zum Jahr 2040 weiterhin wachsen kann. Die Zahl der Zweifler wächst allerdings: Ende 2014 veröffentlichten texanische Geologen eine Untersuchung, nach der das Fördermaximum bereits 2020 erreicht werden könnte.

In Europa hat sich die Technologie jedoch nicht durchgesetzt. Frankreich hat Fracking 2013 verboten. In Deutschland wird die Abstimmung über einen Gesetzentwurf, der Fracking unter scharfen Umweltauflagen ermöglichen würde, immer wieder verschoben. Und aus Polen, das in Europa die größten Lagerstätten haben soll, haben sich Investoren wegen des niedrigen Ölpreises, neuen Abschätzungen zur verfügbaren Menge und Schwierigkeiten mit der Bürokratie wieder zurückgezogen.

WOLFGANG STIELER

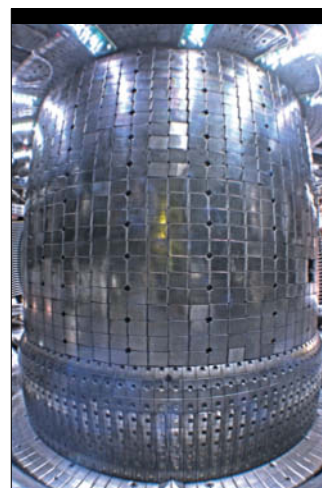


Foto: Wikipedia, Mike Garrett

Technology Review

IN DER NÄCHSTEN AUSGABE LESEN SIE:

UNENDLICHE ENERGIE?

Schneller als Iter: Start-ups versprechen Fusionsenergie schon in fünf Jahren.

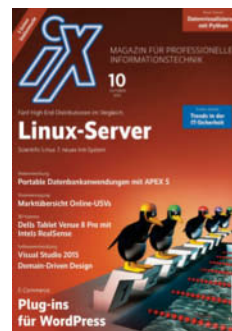
SMART SHOPPING

Führt Online-Shopping zu sterbenden Innenstädten?

AB 22. 10. 2015 IM HANDEL



Ab jetzt im Handel



Ab jetzt im Handel



Ein Missgeschick führte 1865 zur Erfindung des ersten Kunststoffs.

Billard mit Knalleffekt

Wie in vielen Hausapotheken Mitte des 19. Jahrhunderts stand auch in der von John Wesley Hyatt eine Flasche Kollodium. Die zähflüssige Mischung aus Cellulosenitrat („Schießbaumwolle“), Ether und Alkohol diente normalerweise dazu, kleine Hautabschürfungen mit einem durchsichtigen Wundverband zu schützen. Irgendwann im Jahr 1863 stieß Hyatt versehentlich die Flasche um. Weil er die Masse nicht sofort aufwischte, trocknete sie ein – und brachte ihn auf eine Idee, die sein Leben verändern sollte.

Drei Jahre zuvor hatte die Firma Phelan & Collendar, ein Hersteller von Billardkugeln, per Zeitungsannonce ein Preisgeld von 10 000 Dollar für einen preiswerten Elfenbein-Ersatz ausgelobt. Den gelernten Drucker Hyatt und seinen Bruder Isaiah lockte das Preisgeld.

Zunächst versuchten sie, Kugeln aus Papierschnitzeln, Sägemehl und Leim zu formen. Aber sie waren nicht hart genug. Dann aber fiel Hyatt die Flasche Kollodium um. Nach etlichen Versuchen schuf Hyatt damit tatsächlich die erste brauchbare Billardkugel ohne Elfenbein.

Am 10. Oktober 1865 erhielt er dafür das US-Patent 105338, in dem die Rezeptur beschrieben ist: Man löse Cellulosenitrat in Wasser und zermahle es zu einem Brei. Dazu mische man Kampfer – ein aus dem Kampferbaum gewonnenes aromatisches Pulver – und backe das Gemisch unter hohem Druck bei 60 bis 110 Grad Celsius. Fertig war „Celluloid“, das erste thermoplastische Polymer der Geschichte.

Um einen wirklichen „Kunststoff“ handelt es sich dabei streng genommen nicht – schließlich liefert das natürliche Kettenmolekül Cellulose das Grundgerüst. Werden ihm per Salpetersäure NO_2 -Gruppen angehängt, entsteht daraus Schieß-

baumwolle. Mit der eigentlichen Polymerisation haben die weiteren Verarbeitungsschritte hin zum Celluloid nichts mehr zu tun. Der Kampfer dient nur als Weichmacher. Je nach Kampferanteil verhält sich das Celluloid wie Gummi oder wie Horn.

Ob die Gebrüder Hyatt das Preisgeld bekamen, lässt sich nicht mit Sicherheit klären. Möglicherweise wurde es ihnen verweigert, weil sie mit der „Albany Billiard Ball Company“ eine Konkurrenzfirma gründeten. Denkbar ist auch, dass die Stifter den brisanten Hauptbestandteil der Kugeln monierten: die Schießbaumwolle. „Manchmal führt ein heftiger Zusammenprall der Kugeln zu einer leichten Explosion, wie bei einem Zündhütchen“, so Hyatt. Ein Besitzer eines Billardsalons in Colorado berichtete, diese Explosionen seien ihm gleichgültig, nur ziehe jeder Mann im Raum im selben Augenblick seinen Revolver.

Aber Celluloid hatte noch andere Talente: Es nahm bereitwillig Farben an und erlaubt wie kein anderer Werkstoff eine Vielzahl von Maserungen und Strukturen. Zudem ließ es sich hervorragend bearbeiten und in heißem Wasser verformen. So bot es sich an als fast perfekte Nachahmung für Elfenbein, Horn, Schildpatt, Perlmutter oder Koralle, aus denen sich Käämme, Accessoires, Schälchen, Brillengestelle und vieles mehr machen ließ. Hinzu kamen neue Anwendungsgebiete wie abwaschbare Hemdkragen oder Gaumenplatten für künstliche Gebisse. Zur Herstellung konstruierte Hyatt einen Vorläufer heutiger Spritzgießmaschinen. Celluloid wurde zum Selbstläufer und Hyatt zum Millionär.

Im Jahr 1884 meldete dann ein gewisser Georg Eastman, Chef des Kodak-Konzerns, den fotografischen Film aus Celluloid zum Patent an. 1895 liefen die ersten Zelluloidstreifen durch Filmkameras und hielten bewegte Bilder fest. Bis etwa 1951 wurde Filmmaterial auf Nitrozellulosebasis hergestellt. Es hatte hervorragende optische Eigenschaften und eine lange Lebensdauer – solange es nicht entflammte. Da es aber leicht entzündlich war, zerstörte das Material viele Kinos und ganze Filmarchive. Heute fällt es unter das Gesetz über explosionsgefährliche Stoffe.

Da immer weniger Versicherungen bereit sind, eine Celluloid-Fabrik zu versichern, sinkt die Produktion entsprechend. Ein letztes Refugium ist der Sport: Tischtennisbälle bestehen nach wie vor aus Celluloid. Doch auch hier ist ein Ende abzusehen: Der Weltverband ITTF hat im Jahr 2014 auch Bälle aus anderen Kunststoffen erlaubt, damit die Sportler nicht irgendwann ohne Spielmaterial dastehen.

Wegen der schlechten Temperaturbeständigkeit ging die Suche nach einem robusteren Kunststoff schon zu Hyatts Zeiten los. 1910 entwickelte der belgische Chemiker Leo Baekeland das erste vollsynthetische Polymer: Bakelit. Seitdem wird Bakeland fälschlicherweise oft als Urvater des Kunststoffs bezeichnet. Doch das Tor zum Plastikzeitalter hatte Hyatt schon ein halbes Jahrhundert früher aufgestoßen. JOSEPH SCHEPPACH

Foto: Interfoto



Foto: Daniel Reinhardt/ Dpa Picture-Alliance



Foto: Syracuse University

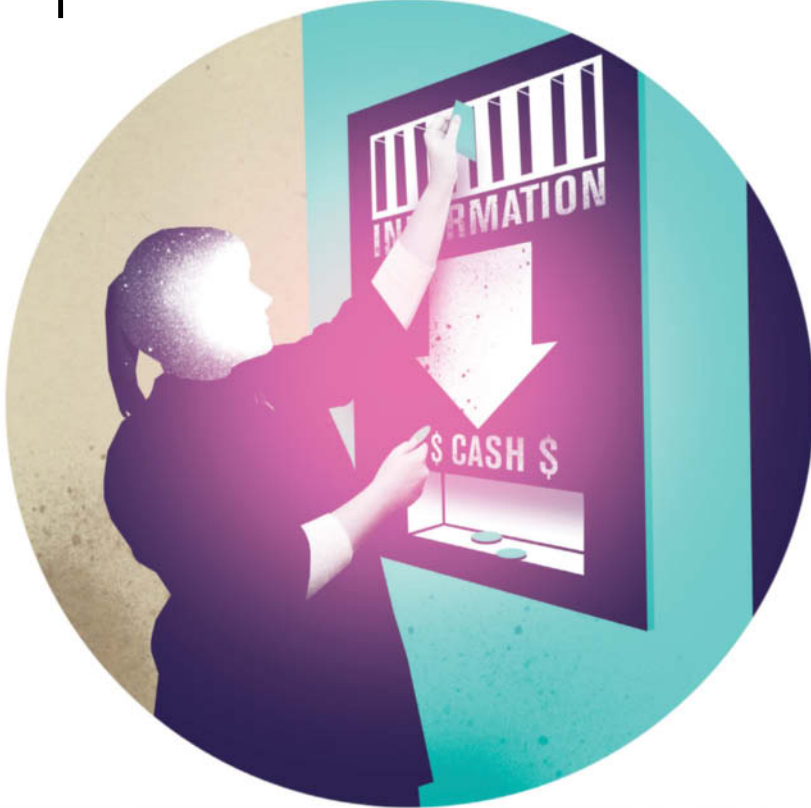


Oben links: Der gelernte Drucker John Wesley Hyatt erfand den ersten thermoplastischen Kunststoff – für Billardkugeln ohne Elfenbein.
Oben rechts: Filmstreifen aus dem Ersten Weltkrieg. Er zeigt französische Soldaten beim Marschieren. Unten: Im Sommer 1959 lagen Filmrollen aus Celluloid auf dem Hof der Cinémathèque française bereit zur Abholung. Die heiße Sonne reichte, um sie zu entzünden.



DER FUTURIST

Spam vom Staat



Was wäre, wenn wir Geld für unsere Daten bekämen?

Nach der Bundestagswahl 2017 wollte die Große Koalition endlich mal wieder ein großes Rad drehen. Diesmal sollte es keinen Spott über #Neuland geben, kein Gemäkel über den immer noch schleppenden Breitbandausbau. Deutschland sollte das ambitionierteste Datenschutzrecht der Welt bekommen – und die Nutzer endlich einen Anteil an dem Geld, das andere mit ihren Daten verdienen.

Also gründete Andrea Voßhoff, Chefin des neu gegründeten Ministeriums für Digitales, zunächst einmal eine weitere Behörde: Die Datengebüreneinzugszentrale (DaGeBüz). Sie stellte jedem Bürger eine Art Datensafe zur Verfügung. Dort waren Stammdaten wie Name, Geburtsdatum, Adresse, Steuer- und Sozialversicherungsnummer automatisch hinterlegt. Nutzer

konnten sie beliebig um Hobbys, Vorlieben, Vereinszugehörigkeiten oder Ähnliches ergänzen. Über entsprechende Schnittstellen konnten sie zudem alle Daten importieren, die soziale Netzwerke, Einkaufsplattformen, Suchmaschinen und Kreditscorer über sie gesammelt haben.

Damit die großen Datenkonzerne mitspielen – eine Zwangsverpflichtung schloss sich wegen der komplizierten internationalen Rechtslage aus –, setzte Voßhoff die DaGeBüz als öffentlich-private Partnerschaft auf. Schnell merkten Facebook, Google und Amazon, dass sie so weitaus bessere Daten bekamen, als sie je selbst sammeln konnten. Da war es verschmerzbar, dass sie 30 Prozent ihres Datenumsatzes an die Bürger abtreten mussten. Ein weiteres Drittel fraßen die Verwaltungsgebühren auf, denn die DaGeBüz wuchs schnell auf eine hohe vierstellige Mitarbeiterzahl und musste in die leer stehenden Gebäude des Flughafens

Berlin-Brandenburg umziehen. Allerdings verdienten die Konzerne in jedem Fall mit, weil sie dank der öffentlich-privaten Partnerschaft auch an der bürokratischen Abwicklung beteiligt waren.

Ein weiterer Teil der Einnahmen wanderte in den Bundeshaushalt, wo er eigentlich den Breitbandausbau finanzieren sollte. Doch dann tat sich in der Rentenkasse ein unerwartet tiefes Loch auf und verschob die Haushaltsprioritäten.

Die Bürger merkten an der Umstellung vor allem, dass sie noch mehr Spam und Werbung bekamen. Kommerzielle Spam-Filter waren machtlos, denn die DaGeBüz hatte mit den Providern und Softwareherstellern ausgehandelt, dass von ihr autorisierte Mails auf jeden Fall zugestellt wurden.

Theoretisch konnten Bürger zwar per Opt-out die Verwertung ihrer Daten untersagen. Doch dazu brauchten sie ein Lesegerät für den elektronischen Personalausweis. Die Nachfrage nach solchen Geräten stieg massiv, während sie zuvor mangels sinnvoller Nutzung jahrelang vor sich hin gedümpelt war. Die wenigen verbliebenen Hersteller kamen nicht mehr mit der Produktion hinterher.

Wer die Werbeflut – freiwillig oder unfreiwillig – über sich ergehen ließ, konnte sich immerhin über ein Taschengeld von fünf bis zehn Euro im Monat freuen. Unter Teenagern wurde es zum Sport, die Portale mit echten oder erfundenen Daten zu füttern, um eine möglichst hohe Auszahlung zu erreichen. In einschlägigen Foren machten schnell Tipps die Runde, welche angeblichen Hobbys am lukrativsten waren. Doch nach einer gewissen Zeit durchschauten die Algorithmen der DaGeBüz solche Fakes, indem sie Daten aus unterschiedlichen Quellen abglich. Dann sperrten sie sämtliche Auszahlungen für einen Monat, bei Wiederholungsfällen auch länger.

Kanzlerin Merkel war dennoch zufrieden: Die notorisch verschnarchte deutsche Netzpolitik galt plötzlich als wegweisend. Überall auf der Welt gründeten Staaten Datenzentralen nach dem Vorbild der DaGeBüz.

GREGOR HONSEL

iX Payment-Konferenz 2015



**SAVE
THE DATE**
1. Dezember 2015,
Frankfurt

Einfach bezahlen – mobil, im Netz, im Laden

Eine Welt ohne Banken und Bargeld? Das Smartphone löst die Geldbörse ab – Fintech Startups und Kryptowährungen wie Bitcoin rütteln am etablierten Finanzsystem. Die Branche ist im Umbruch.

Die iX Payment-Konferenz 2015 nimmt Technik, Verfahren und Konzepte unter die Lupe und beleuchtet die Umsetzung in der Praxis.

Frühbuchergebühr: 405,00 Euro (inkl. MwSt.)

Standardgebühr: 450,00 Euro (inkl. MwSt.)

THEMEN:

- Mobile Payment – Systeme im Vergleich
- Bezahlverfahren im internationalen B2B-E-Commerce
- Kontaktlos und mobil bezahlen in Deutschland
- Krypto-Währungen – Die Bitcoin-Akzeptanz wächst
- Erfahrungsbericht: Leben ohne Bargeld
- Datenschutz – Gläserne Kunden durch digitale Geldbörsen und soziale Vernetzung?

Eine Veranstaltung von:



Organisiert von:



Weitere Informationen und Anmeldung unter: www.heise-events.de/payment2015

Nutzen Sie die Möglichkeit zur PGP-Zertifizierung: www.ct.de/pgp



Auch auf der Datenautobahn vorn.

Auf Wunsch bietet Ihnen die App „Volkswagen Car-Net e-Remote“ via Smartphone Zugriff auf viele hilfreiche Fahrzeugfunktionen – und zeigt Ihnen zum Beispiel das Ladelevel und die verbleibende Reichweite an.

Der neue Passat GTE Variant.

Think New.



17. – 27. September
Frankfurt am Main

Mehr erfahren auf www.volkswagen.de/passatgte



Das Auto.

Kraftstoffverbrauch in l/100 km: kombiniert 1,7–1,6, Stromverbrauch in kWh/100 km: kombiniert 12,9–12,4,
CO₂-Emissionen in g/km: kombiniert 39–37. Abb. zeigt optionale Sonderausstattung.